WHAT'S NEW IN THIS REVISED SECTION

Effective July 2006, footnote 3 was revised to include a reference to SR-00-14, "Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign 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. 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 docu-

1. Appendix A defines these primary risk types.

mented). 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 section 4070.1 and SR-95-51.)

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 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 com-

2. Guidance on the selection of loans for review is provided in SR-94-13, "Loan Review Requirements for On-Site Examinations."

petence 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.

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-

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."

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 January 2009, this section has been revised to include additional risk-focused SR letter topics and manual references in appendix A.

2124.01.1 INSPECTION APPROACH FOR RISK-FOCUSED SUPERVISION

The inspection approach for large complex banking organizations (LCBOs) is a risk-focused process that relies on (1) an understanding of the banking organization[1] (the institution), (2) the performance of risk assessments, (3) the development of a supervisory plan, and (4) inspection procedures that are tailored to the risk profile. The process for a complex institution relies more heavily on a central point of contact (CPC), detailed risk assessments, and a supervisory plan before the on-site inspection. The risk-focused inspection also incorporates the U.S. operations of foreign banking organizations (FBOs), for which the Federal Reserve has overall supervisory authority. See SR-97-24, SR-99-15, and section 2124.04.

2124.01.1.1 Risk-Focused Supervisory Objectives

The Federal Reserve is committed to ensuring that the supervisory process for all banking organizations under its purview meets the following objectives:

1. *To provide flexible and responsive supervision.* The supervisory process is designed to be dynamic and forward-looking so that it responds to technological advances, product innovation, and new risk-management systems and techniques, as well as to changes in the condition of an individual financial institution and developments in the market.
2. *To foster consistency, coordination, and communication among the appropriate supervisors.* Seamless supervision, which reduces regulatory burden and duplication, is promoted. The supervisory process uses examiner resources effectively by using the institution's internal and external risk-assessment and risk-monitoring systems; making appropriate use of joint and alternating examinations and inspections; and tailoring supervisory activities to an institution's condition, risk profile, and unique characteristics.
3. *To promote safety and soundness.* The supervisory process effectively evaluates the safety and soundness of banking organizations, including the assessment of risk-management systems, financial condition, and compliance with laws and regulations.
4. *To provide a comprehensive assessment of the institution.* The supervisory process integrates specialty areas (for example, information technology systems, trust, capital markets, and consumer compliance (see SR-03-22/CA-03-15)) and functional risk assessments and reviews, in cooperation with interested supervisors, into a comprehensive assessment of the institution.

2124.01.1.2 Key Elements of the Risk-Focused Framework

To meet the established objectives and respond to the characteristics of large institutions, the framework for risk-focused supervision of large complex institutions contains the following key elements:

1. *Designation of a central point of contact.* Large institutions typically have operations in several jurisdictions, multiple charters, and diverse product lines. Consequently, the program requires that a CPC be designated for each institution to facilitate coordination and communication among the principal bank and other regulatory authorities (for example, securities, insurance, and other nonbanking supervisory entities). Further, the program requires that each CPC and LCBO be assigned a dedicated supervisory team and staff with specialized skills, knowledge, and experience tailored to the unique profile of a particular institution.
2. *Review of functional activities.* Large institutions are generally structured along business

1. For this section, the term *banking organization* refers to bank holding companies (BHCs) and their domestic and foreign banking and nonbank subsidiaries. It is used synonomously with the term *institutions.* That term, however, has an even broader meaning since it may include other entities (for example, Edge Act corporations and foreign branches of state member banks). See section 2124.01.1.3.1.

lines or functions, and some activities are managed on a centralized basis. As a result, a single type of risk may cross several legal entities. Therefore, the supervisory program incorporates assessments along functional lines to evaluate risk exposure and its impact on safety and soundness. These functional reviews will be integrated into the risk assessments for specific legal entities and used to support the supervisory ratings for individual legal entities.[2]

3. *Focus on risk-management processes.* Large institutions generally have highly developed risk-management systems, such as internal audit, loan review, and compliance. The supervisory program emphasizes each institution's responsibility to be the principal source for detecting and deterring abusive and unsound practices through adequate internal controls and operating procedures. The program incorporates an approach that focuses on and evaluates the institution's risk-management systems, processes, and core proficiencies for identifying, measuring, monitoring, and controlling key risks, including credit, market, and operational risks. Yet, the program retains transaction testing and supervisory rating systems, such as CAMELS, RFI/C(D), and ROCA. This diagnostic perspective provides insight into how effectively an institution is managing its operations and how well it is positioned to meet future business challenges. The program places less emphasis on traditional "point-in-time" balance-sheet assessments.
4. *Tailoring of supervisory activities.* Large institutions are unique, but all possess the ability to quickly change their risk profiles. To deliver effective supervision, the program incorporates an approach that tailors supervisory activities to the risk profile of an institution. By concentrating on an institution's major risk areas, examiners can achieve a more relevant and penetrating understanding of the institution's condition.
5. *Review of internally and externally generated management information.* A review of internal management and board reports, internal and external audit reports, and publicly available information will further supplement existing supervisory processes. Banking organizations are also encouraged to continually review and enhance their public disclosures in order to promote transparency and to foster and support supervisory processes and effective market discipline.
6. *Emphasis on ongoing supervision.* Large institutions face a rapidly changing environment. The supervisory program thus emphasizes ongoing supervision, monitoring, and assessment through increased planning; a no-less-than-quarterly reassessment of the organization's profile; and continuous off-site monitoring. Ongoing supervision allows for timely adjustments to the supervisory strategy as conditions change within the institution, enhanced information sharing Systemwide and on an interagency basis, and the use of information technology platforms that foster more-effective collaboration and communication.
7. *Effective communication with management.* An effective program of regular and meaningful contacts with management is necessary to maintain a current understanding of the institution's risk profile and risk-management processes without imposing undue burden, interfering with legitimate management prerogatives, or compromising the objectivity of the supervisory process.

2124.01.1.3 Banking Organizations Covered by the Framework

For purposes of the risk-focused supervision framework, LCBOs generally have a functional-management structure, a broad array of products, operations that span multiple supervisory jurisdictions, and consolidated assets of $1 billion or more.[3] These institutions may be state member banks, BHCs (including their nonbank and foreign subsidiaries), and branches and agencies of FBOs. The complex-institution process may also be appropriate for some organizations with consolidated assets less than $1 billion.

LCBOs are larger institutions that have particularly complex operations and dynamic risk profiles. To be effective, a supervisory program

2. When functions are located entirely in legal entities that are not primarily supervised by the Federal Reserve, the results of supervisory activities conducted by the primary regulator will be used to the extent possible to avoid duplication of activities.

3. Large institutions are defined differently in other regulatory guidance regarding regulatory reports and examination mandates.

for LCBOs requires a heightened level of planning, coordination, and innovative techniques. These organizations typically have significant on- and off-balance-sheet risk exposures, offer a broad range of products and services at the domestic and international levels, are subject to multiple supervisors in the United States and abroad, and participate extensively in large-value payment and settlement systems.

An important aspect of the LCBO program is the assessment and evaluation of banking practices across a group of institutions with similar business lines, characteristics, and risk profiles. This ''portfolio'' approach to supervision will (1) support and enhance timely judgments about individual institutions, including the identification of possible ''outliers''; (2) facilitate peer-group assessments; (3) provide an improved framework for discerning industry trends; (4) foster more-consistent supervision of institutions with similar businesses and risk profiles; (5) contribute substantially to the maintenance of a highly informed and skilled supervisory staff; and (6) promote the development and sharing of the best supervisory practices within the Federal Reserve and the supervisory community more broadly.

2124.01.1.3.1 Foreign Institutions

U.S. supervisory authorities are host-country rather than home-country supervisors for most of the U.S. operations of FBOs; therefore, the supervisory focus and objectives are somewhat different for U.S. operations of FBOs and are addressed separately in the FBO supervision program. The desired result of a risk-focused examination process, however, should be the same. The framework encompasses the supervision and examination processes and procedures relevant to the U.S. operations of FBOs, to the extent that they are appropriate. Any significant remaining differences are incorporated in the FBO supervision program.

2124.01.1.3.2 Nonbank Subsidiaries of Domestic Institutions

Nonbank subsidiaries of large complex domestic institutions are covered by the risk-focused supervision program. These subsidiaries include (1) nonbank subsidiaries of the parent bank holding company and those of the subsidiary state member banks; (2) the significant branch operations, primarily foreign-branch operations, of state member banks; and (3) subsidiary foreign banks of the holding company. The level of supervisory activity to be conducted for nonbank subsidiaries and foreign branches and subsidiaries of domestic institutions should be based on their individual risk levels relative to the consolidated organization. The risk associated with significant nonbank subsidiaries or branches should be identified as part of the consolidated risk-assessment planning process, and the appropriate level of supervisory coverage (whether on- or off-site) should be described in the supervisory plan for the organization. Risk-focused supervisory planning should use the workpaper ''Nonbank Subsidiary of a Bank Holding Company Risk-Assessment Questionnaire'' (see appendix B). It should be used as a guide for (1) determining whether a nonbank subsidiary poses significant risk to the entire LCBO (parent bank holding company) and (2) determining whether an on-site supervisory inspection or examination of the entity is needed.[4] The supervisory plan for the organization should also include a review of the institution's processes to ensure compliance with sections 23A and 23B of the Federal Reserve Act, Regulation W, and various other regulations and guidelines that govern transactions between the bank and nonbank affiliates.

2124.01.1.3.3 Edge Act Corporations

Under section 25A, paragraph 17, of the Federal Reserve Act, Edge Act corporations are subject to examination once a year and at such other times as deemed necessary by the Federal Reserve. While Reserve Banks must fulfill this legal mandate, there is flexibility in determining the extent of examination coverage. The scope of Edge Act corporation examinations should be determined through the risk-assessment process. Additionally, separate reports of examination are not required for Edge Act corporations, provided that all relevant findings are included in the consolidated report of examination of the

4. When this workpaper is used, a separate risk assessment of each nonbank subsidiary of the LCBO (for domestic bank holding companies) is not required. The separate-risk-assessment requirements of SR-93-19 are thus partially superseded for LCBOs. Nonbank subsidiary risk assessments should be reflected in the entire consolidated organization's risk assessment.

parent bank.[5] This reporting procedure also applies to other nonbank subsidiaries of the bank or bank holding company.

2124.01.1.3.4 Specialty Areas Covered by the Framework

The Federal Reserve regularly conducts examinations, inspections, or reviews of several specialty areas. To achieve more-efficient supervision and reduce the regulatory burden on institutions, steps have been taken to coordinate these reviews with the annual full-scope inspection of the consolidated organization. Under the risk-focused approach, the specialty areas should be included in the planning process in relation to the perceived level of risk to the consolidated organization or any state member bank subsidiary. Reviews of any specialty areas can be performed in conjunction with the annual full-scope inspection, or through targeted examinations or inspections, at any time during the supervisory cycle. The findings of all specialty reviews should be included in the inspection report for the consolidated organization.

2124.01.2 COORDINATION OF SUPERVISORY ACTIVITIES

Many large complex institutions have interstate operations that expand with the continuation of mergers and acquisitions. In this environment, close cooperation with the other federal and state banking agencies is critical. To facilitate coordination between the Federal Reserve and other regulators, district Reserve Banks have been assigned roles and responsibilities that reflect their status as the responsible Reserve Bank (RRB).

2124.01.2.1 Responsible Reserve Bank

The RRB facilitates the increased flexibility, planning, and coordination needed to effectively and efficiently supervise institutions with interstate operations. Considering the overriding objectives of seamless risk-focused supervision, the RRB is responsible for designating the CPC and for ensuring that all aspects of the supervisory process are fully coordinated with LRBs and home-state supervisors. Close coordination among the other appropriate regulators for each organization is critical to ensure a consistent risk-focused approach to supervision.

2124.01.2.2 RRBs Working with Local Reserve Banks

The RRB is accountable for all aspects of the supervision of a fully consolidated banking organization, which includes the supervision of all the organization's subsidiaries and affiliates (domestic, foreign, and Edge corporations) for which the Federal Reserve has supervisory oversight responsibility. The RRB is generally expected to work with local Reserve Banks (LRBs) in conducting examinations (and inspections) and other supervisory activities, particularly where significant banking operations are conducted in a local District. Thus, for state member banks, the LRB has an important role in the supervision of that subsidiary. However, the RRB retains authority and accountability for the results of all examinations, inspections, and reviews that an LRB may perform on its behalf.

2124.01.2.2.1 RRB Defined

In general, the RRB for a banking organization has been the Reserve Bank in the District where the banking operations of the organization are principally conducted. For domestic banking organizations, the RRB typically will be the Reserve Bank District where the head office of the top-tier organization is located and where its overall strategic direction is established and overseen. For foreign banking organizations, the RRB typically will be the Reserve Bank District where the Federal Reserve has the most direct involvement in the day-to-day supervision of the U.S. banking operations of the organization.

When necessary, the Board's Division of Banking Supervision and Regulation (BS&R), in consultation with the Division of Consumer and Community Affairs (C&CA), may designate an RRB when the general principles set forth above could impede the ability of the Federal Reserve to perform its functions under law, do not result in an efficient allocation of supervisory resources, or are otherwise not appropriate. When more than one Reserve Bank currently shares supervisory responsibilities for

5. A separate memorandum to the file should be prepared and retained. The memorandum should provide the date of examination of the Edge Act corporation, a summary of findings, the rating assigned, and a reference to the consolidated report of examination. This information should also be forwarded to Federal Reserve Board staff.

a consolidated banking organization, Board staff will work with Reserve Bank staff to determine the RRB.

2124.01.2.2.2 Duties of RRBs

The RRB develops the consolidated risk assessment and supervisory plan and ensures that the scope and timing of planned activities conducted by participating Districts and agencies pursuant to the plan are appropriate, given the consolidated risk assessment. The RRB designates the central point of contact or lead examiner and ensures that all safety-and-soundness, information technology, trust, consumer compliance, Community Reinvestment Act (CRA), and other specialty examinations (and inspections) and visitations are conducted and appropriately coordinated within the System and with other regulators. In addition, the RRB manages all formal communications with the foreign and domestic supervised entity, including the communication of supervisory assessments, ratings, and remedial actions.[6]

2124.01.2.2.3 Sharing of RRB Duties

To take advantage of opportunities to enhance supervisory effectiveness or efficiency, an RRB is encouraged to arrange for the LRB to undertake on its behalf certain examinations or other supervisory activities. For example, a local District may have relationships with local representatives of the organization or local supervisors; leveraging these relationships may reduce cots or facilitate communication. Additionally, LRBs may provide specialty examination resources—in the case of CRA examinations, LRB staff often provide valuable insights into local communities and lending institutions that should be factored into the CRA assessment. When other Reserve Bank Districts conduct examinations, inspections, and other supervisory activities for the RRB, substantial reliance should be placed on the conclusions and ratings recommended by the participating Reserve Bank(s).

The RRB retains authority and accountability for the results of all examinations and reviews performed on its behalf and, therefore, must work closely with LRB examination teams to ensure that examination scopes and conclusions are consistent with the supervisory approach and message applied across the consolidated organization. If an LRB identifies major issues in the course of directly conducting supervisory activities on behalf of an RRB, those issues should be brought to the attention of the RRB in a timely manner.

If an RRB arranges for an LRB to conduct supervisory activities on its behalf, the LRB is responsible for the costs of performing the activities. If the LRB is unable to fulfill the request from the RRB to perform the specified activities, the RRB should seek System assistance, if needed, by contacting Board staff or using other established procedures for coordinating resources.

2124.01.2.3 Central Point of Contact

A CPC is critical to fulfilling the objectives of seamless risk-focused supervision. The RRB should designate a CPC for each large complex institution it supervises. Generally, all Federal Reserve System contacts, activities, and duties, as well as those conducted with other supervisors, should be coordinated through this contact. The CPC should—

1. be knowledgeable, on an ongoing basis, about the institution's financial condition, management structure, strategic plan and direction, and overall operations;
2. remain up-to-date on the condition of the assigned institution and be knowledgeable regarding all supervisory activities, monitoring and surveillance information, applications issues, capital-markets activities, meetings with management, and enforcement issues, if applicable;
3. ensure that the objectives of seamless risk-focused supervision are achieved for each institution and that the supervisory products (that is, an institutional overview, a risk matrix, a risk assessment, a supervisory plan, an inspection program, a scope memorandum, inspection modules, and an inspection report) are prepared in a timely manner;
4. ensure appropriate follow-up and tracking of supervisory concerns, corrective actions, or other matters that come to light through ongoing communications and/or surveillance; and
5. participate in the inspection or examination process, as needed, to (1) ensure consistency

6. Additional guidance on inter-District coordination and supervisory responsibilities can be found in section 2124.04; SR-97-24, "Risk-Focused Framework for Supervision of Large Complex Institutions"; and SR-96-33, "State/Federal Protocol and Nationwide Supervisory Agreement."

with the institution's supervisory plan and effective allocation of resources, including coordination of on-site efforts with specialty examination areas and other supervisors, as appropriate, and (2) facilitate requests for information from the institution, wherever possible.

2124.01.2.4 Sharing of Information

To further promote seamless risk-focused supervision, information related to a specific institution should be provided, as appropriate, to other interested supervisors. Sharing of these products with the institution, however, should be carefully evaluated on a case-by-case basis. The institutional overview, risk assessment, and supervisory plan may not be appropriate for release if they contain a hypothesis about an institution's risk rather than assessments verified through the inspection or examination process. On the other hand, it may be appropriate to share the inspection program with the institution in the interest of better coordination of activities.

2124.01.2.5 Coordination with Other Supervisors

Section 305 of the Riegle Community Development and Regulatory Improvement Act of 1994 directed the agencies to coordinate their examinations, to the extent possible, when they are jointly responsible for the examination of various entities of a bank holding company.[7] To help achieve the desired degree of coordination, staffs of the agencies are expected, primarily at the regional level, to discuss examination plans and coordination issues. The institution involved is to be kept fully informed of the coordinated activities planned by the agencies, including a general time frame of when each agency expects to conduct its examination activities.

2124.01.3 FUNCTIONAL APPROACH AND TARGETED INSPECTIONS

The framework for risk-focused supervision of large complex institutions relies more heavily on a functional-business-line approach to supervising institutions, while effectively integrating the functional approach into the legal-entity assessment. Bank holding companies are increasingly being managed on a functional basis. Functional management allows organizations to take advantage of the synergies among their components, deliver better products to the market, and provide higher returns to stockholders. Virtually all of the large bank holding companies operate as integrated units and are managed as such. For these companies, the risk-management systems are generally organized along business lines on a centralized basis. A key implication of this shift in management structure is that much of the information and insight gathered on inspections and examinations of individual legal entities can be fully understood only in the context of examination findings of other related legal entities or centralized functions. Developing that understanding means adapting some of the same functional-business-line approaches to supervision, including examination processes. Consequently, the risk-focused supervision framework incorporates risk assessments, that is, inspection and examination procedures that are organized by function.

The functional approach focuses principally on the key business activities (for example, lending, treasury, retail banking) rather than reviewing the legal entity and its balance sheet. This does not mean that the responsibility for a legal-entity assessment is ignored, nor should the Federal Reserve perform examinations of institutions for which other regulators have primary supervisory responsibility.[8] Rather, Federal Reserve examiners should integrate the findings of a functional review into the legal-entity assessment and should coordinate closely with the primary regulator to gather sufficient information to form an assessment of the consolidated organization. Nonetheless, in some cases, effective supervision of the consolidated organization may require Federal Reserve examiners to perform process reviews and, possibly, transaction testing at all levels of the organization.

Functional-risk-focused supervision is to be achieved by the following actions:

7. In a December 1996 letter to the House Committee on Banking and Financial Services, the agencies outlined their cooperative efforts to meet the objectives of section 305.

8. With respect to U.S. banks owned by FBOs, it is particularly important to review the U.S. bank on a legal-entity basis and also the risk exposure to the U.S. bank from its parent foreign bank, as U.S. supervisory authorities do not supervise or regulate the parent bank.

1. Planning and conducting joint inspections and examinations with the primary regulator in areas of mutual interest, such as nondeposit investment products, interest-rate risk, liquidity, and mergers and acquisitions.
2. Leveraging off, or working from, the work performed by the primary regulator and the work performed by the institution's internal and external auditors by reviewing and using their workpapers and conclusions to avoid duplication of effort and to lessen the burden on the institution.
3. Reviewing inspection and examination reports and other communications to the institution that were issued by other supervisors.
4. Conducting a series of functional reviews or targeted inspections or examinations of business lines, relevant risk areas, or areas of significant supervisory concern during the supervisory cycle.[9] Functional reviews and targeted inspections or examinations are increasingly necessary to evaluate the relevant risk exposure of a large complex institution and the effectiveness of related risk-management systems.

The relevant findings of functional reviews or targeted inspections and examinations should be handled as outlined below.

1. *Incorporated into the annual full-scope inspection.* In this context, a full-scope inspection involves the analysis of data sufficient to determine the safety and soundness of the institution and to assign supervisory ratings. The inspection or examination procedures required to arrive at those determinations do not necessarily have to be performed at the time of the annual inspection; they can be a product of the collective activities performed throughout the supervisory cycle. However, inspection procedures should include follow-up for deficiencies noted in functional reviews or targeted inspections and examinations.
2. *Conveyed to the institution's management during a close-out or exit meeting with the relevant area's line management.* The need to communicate the findings to senior management or the board of directors is left to the judgment of Reserve Bank management, based on the significance of the findings.
3. *Communicated in a formal written report to the institution's management or board of directors when significant weaknesses are detected or when the findings result in a downgrade of any rating component.* Otherwise, the vehicle for communicating the results is left to the judgment of the Reserve Bank's management and may either be a formal report or a supervisory letter.[10]

The functional approach to risk assessments and the planning of supervisory activities should include a review of the parent company and its significant nonbank subsidiaries. However, it is anticipated that the level of supervisory activities, on- or off-site, will be appropriate to the risk profile of the parent company or its nonbank subsidiary in relation to the consolidated organization. Intercompany transactions should continue to be reviewed as part of the inspection procedures performed, to ensure that they comply with laws and regulations and do not pose safety-and-soundness concerns.

2124.01.4 OVERVIEW OF THE PROCESS AND PRODUCTS

The risk-focused methodology for the supervision program for large complex institutions reflects a continuous and dynamic process. As table 1 indicates, the methodology consists of six key steps, each of which uses certain written products to facilitate communication and coordination.

9. A supervisory cycle is the period of time from the close of one annual examination to the close of the following annual examination.

10. As discussed in SR-99-17, it is Federal Reserve System practice to update RFI/C(D) ratings between inspections to keep them current and to ensure that they reflect the latest information on the institution's financial condition. For state member banks, Reserve Banks are to refrain from revising CAMELS ratings based on off-site analysis in view of the emphasis being placed on the CAMELS ratings for implementing risk-based insurance assessments and other supervisory initiatives. In accordance with SR-99-17 (see also section 5010.4), Reserve Banks should notify the institution's management whenever the rating is changed as a result of off-site analysis.

Table 1—Steps and Products Involved in the Risk-Focused Supervision Process

Steps	*Products**
1. Understanding the institution	1. Institutional overview
2. Assessing the institution's risk	2. Risk matrix 3. Risk assessment
3. Planning and scheduling supervisory activities	4. Supervisory plan 5. Inspection/examination program
4. Defining inspection activities	6. Scope memorandum 7. Entry letter
5. Performing inspection procedures	8. Functional-inspection modules
6. Reporting the findings	9. Inspection report(s)

* For examples of products 1 through 8, see appendixes D through K of the Federal Reserve's handbook "Framework for Risk-Focused Supervision of Large, Complex Institutions," referred to in SR-97-24. See also appendix B, the bank holding company nonbank subsidiary risk-assessment questionnaire, which is discussed in section 2124.01.1.3.2.

With the exception of the entry letter, the written products associated with steps 1 through 4 are designed to sharpen the supervisory focus on an institution's business activities that pose the greatest risk, as well as to assess the adequacy of the institution's risk-management systems to identify, measure, monitor, and control risks. The products should be revised as new information is received from such sources as the current inspection, recent targeted inspections and examinations, and periodic reviews of regulatory reports.

The focus of the products should be on fully achieving a risk-focused, seamless, and coordinated supervisory process. The content and format of the products are flexible and should be adapted to correspond to the supervisory practices of the agencies involved and to the structure and complexity of the institution.

2124.01.5 UNDERSTANDING THE INSTITUTION

The starting point for risk-focused supervision is developing an understanding of the institution. This step is critical to tailoring the supervision program to meet the characteristics of the organization and to adjusting that program on an ongoing basis as circumstances change. It is also essential to clearly understand the Federal Reserve's supervisory role in relation to an institution and its affiliates. For example, the Federal Reserve's role pertaining to an FBO will vary depending on whether the Federal Reserve is the home- or host-country supervisor for the particular legal entity. Thus, planning and monitoring are key components.

Through increased emphasis on planning and monitoring, supervisory activities can focus on the significant risks to the institution and on related supervisory concerns. Given the technological and market developments within the financial sector and the speed with which an institution's financial condition and risk profile can change, it is critical to keep abreast of events and changes in risk exposure and strategy. The CPC for each large complex institution should continuously review certain information and prepare an institutional overview that will communicate the contact's understanding of that institution.

2124.01.5.1 Sources of Information

Information generated by the Federal Reserve, other supervisors, the institution, and public organizations may assist the CPC in forming and maintaining an ongoing understanding of the institution's risk profile and current condition. For example, the Federal Reserve maintains a significant amount of financial and structure information in various automated databases. In addition, prior inspection and examination reports are excellent sources of information regarding previously identified problems.

Each Reserve Bank has various surveillance reports that identify outliers when an institution is compared with its peer group. The Bank Holding Company Performance Report and the Uniform Bank Performance Report may identify significant deviations in performance relative to institutions' peer groups, currently and between the inspections and examinations of those institutions. For branches and agencies, state member banks, and domestic bank holding companies that are part of FBOs, the strength-of-support assessment (SOSA) rating and relevant credit assessments from major rating agencies provide information that needs to be considered in developing an appropriate supervisory strategy. For FBOs, the Federal Reserve has developed automated systems that provide information on foreign financial systems, for-

eign accounting standards, and the financial performance of FBOs with U.S. operations.

Leveraging off the work, knowledge, and conclusions of other supervisors is of key importance to understanding a large complex organization. Ongoing contact and the exchange of information with other supervisors who have responsibilities for a given institution may provide insights that cannot be obtained from other sources. Additional information can be obtained from examination reports issued by other supervisors and from their databases, for example, the OCC's Supervisory Monitoring System (SMS) and the FDIC's Bank Information Tracking System (BITS).

Using information generated by the institution's management information system improves the supervisory process. It provides an efficient way to reduce on-site time, identify emerging trends, and remain informed about the activities of the institution and financial markets. Information that may be periodically reviewed by the contact includes the size and composition of intra-day balance sheets, internal risk-ratings of loans, internal limits and current risk measures regarding trading activities, and internal limits and measures covering the institution's interest-rate and market risk. Additionally, functional-organization charts reflecting the major lines of business across legal entities, changes to the organization's strategic plan, and information provided to the board of directors and management committees should be reviewed.

The CPC should also hold periodic discussions with the institution's management to cover, among other topics, credit-market conditions, new products, divestitures, mergers and acquisitions, and the results of any recently completed internal and external audits. When other agencies have supervisory responsibilities for the organization, joint meetings should be considered.

Publicly available information may provide additional insight into an institution's condition. This information may be particularly valuable in assessing an organization's ability to raise capital. Public sources of information include SEC reports, press releases, and analyses by private rating agencies and by securities dealers and underwriters.

2124.01.5.2 Preparation of the Institutional Overview

The institutional overview should provide an executive summary that communicates, in one concise document, information demonstrating an understanding of the institution's present condition and its current and prospective risk profiles. The overview should also highlight key issues and past supervisory findings. General types of information that may be valuable to present in the overview are listed below:[10a]

1. a brief description of the organizational structure (with comments on the legal and business units) and changes through merger, acquisition, divestitures, consolidation, or charter conversion since the prior review
2. a summary of the organization's business strategies, key business lines, product mix, marketing emphasis, growth areas, acquisition or divestiture plans, and new products introduced since the prior review
3. key issues for the organization, either from external or internal factors (for example, difficulties in keeping pace with competition or poorly performing business lines)
4. an overview of management, commenting on the level of board oversight, leadership strengths or weaknesses, policy formulation, and the adequacy of management information systems (Comments should include anticipated changes in key management, unusual turnover in line management, and management-succession plans. Key executives and the extent of their participation in strategic planning, policy formulation, and risk management may also be described.)
5. a brief analysis of the consolidated financial condition and trends, including earnings, invested capital, and return on investment by business line
6. a description of the future prospects of the organization, expectations or strategic forecasts for key performance areas, and budget projections
7. descriptions of internal and external audit, including the nature of any special work performed by external auditors during the period under review
8. a summary of supervisory activity performed since the last review, including safety-and-soundness inspections, examinations, and targeted or specialty inspections or

10a. This list is provided in the context of institutions for which the Federal Reserve is the home-country supervisor. In the case of an FBO, the analysis should begin with the SOSA rating and the Summary of Condition of its U.S. operations. See SR-00-14 and also sections 2124.0.2.5, 2127.0, and 3903.0.

examinations; supervisory actions and the institution's degree of compliance; and applications approved or in process
9. considerations for conducting future inspections, including the institution's preference for the coordination of specialty inspections or examinations and combined inspection and examination reports, as well as logistical and timing considerations, including conversion activities, space planning, and management availability

2124.01.6 ASSESSING THE INSTITUTION'S RISKS

In order to focus supervisory activities on the areas of greatest risk to an institution, the CPC or designated staff personnel should perform a risk assessment. The risk assessment highlights both the strengths and vulnerabilities of an institution and provides a foundation for determining the supervisory activities to be conducted. Further, the assessment should apply to the entire spectrum of risks facing an institution, including the following risks:

1. *credit risk,* which arises from the potential that a borrower or counterparty will fail to perform on an obligation
2. *market risk,* which is the risk to an institution's financial condition resulting from adverse movements in market rates or prices, such as interest rates, foreign-exchange rates, or equity prices
3. *liquidity risk,* which is the potential that an institution 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 because it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions (referred to as ''market liquidity risk'')
4. *operational risk,* which 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,* which arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a banking organization
6. *reputational risk,* which is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions

An institution's business activities present various combinations and concentrations of the above risks depending on the nature and scope of the particular activity. When conducting the risk assessment, consideration must be given to the institution's overall risk environment, the reliability of its internal risk management, the adequacy of its information technology systems, and the risks associated with each of its significant business activities. The preparation of the risk matrix provides a structured approach to assessing an institution's risks and is the basis for preparing the narrative risk assessment. See section 4070.1 and SR-95-51 for additional guidance on the evaluation of an institution's risk management.

2124.01.6.1 Assessment of the Overall Risk Environment

The starting point in the risk-assessment process is an evaluation of the institution's risk tolerance and of management's perception of the organization's strengths and weaknesses. Such an evaluation should entail discussions with management and a review of supporting documents, strategic plans, and policy statements. Management, in general, is expected to have a clear understanding of the institution's markets; the general banking, business, and economic environment; and how these factors affect the institution (in other words, their effect on the institution's use of technology, products, and delivery channels).

The institution should have a clearly defined risk-management structure. This structure may be formal or informal, centralized or decentralized. However, the greater the risk assumed by the institution, the more sophisticated its risk-management system should be. Regardless of the approach, the types and levels of risk an institution is willing to accept should reflect the risk appetite determined by its board of directors.

2124.01.6.1.1 Internal-Risk-Management Evaluation

In assessing the overall risk environment, the CPC should make a preliminary evaluation of

the institution's internal risk management. That includes an assessment of the adequacy of the institution's internal audit, loan-review, and compliance functions. External audits also provide important information regarding the risk profile and condition of the institution and may be used in the risk assessment. In completing this evaluation, Reserve Banks should consider holding meetings with the external auditor and senior management who are responsible for internal audit, loan review, and compliance, as well as with other key risk managers. As appropriate, the meetings should be held jointly with a representative from other supervisory agencies that have an interest in the institution.

In addition, the CPC or designated staff personnel should consider reviewing risk assessments developed by the internal audit department for significant lines of business, and then compare their results with the supervisory risk assessment. Further, the CPC should consider evaluating management's ability to aggregate risks on a global basis. Examiners can use this preliminary evaluation to determine how much they can rely on the institution's internal risk management when developing their scope of inspection and examination activities.

2124.01.6.1.2 Supervision Program for Consumer Compliance Risk Assessment at BHCs

Changes in the banking and financial services industry have highlighted the importance of incorporating an assessment of consumer compliance risk into the evaluation of a banking organization's overall risk profile. To address this need, the Federal Reserve enhanced its bank holding company supervision program to ensure that examiners are focusing appropriately on consumer compliance risk–related matters across the broad range of a BHC's activities. (See SR-03-22.)

An enhanced supervisory framework for the supervision of consumer compliance risk was developed for large complex banking organizations (LCBOs) and for large banking organizations (LBOs).[10b] Under the framework, consumer compliance examiners are to assess consumer compliance risk across the broad range of a banking organization's activities to determine the level and trend of consumer compliance risk. To address the risks identified in an organization's business activities, the supervisory team will develop a supervisory plan that includes activities appropriate to the level of the organization's consumer compliance risk.

Supervisory framework for consumer compliance risk. For LCBOs and LBOs that are subject to the System's continuous supervision program, safety-and-soundness examiners are to incorporate an assessment of consumer compliance risk into the overall risk assessment and planned supervisory activities for these organizations. When performing the consumer compliance risk assessment, consumer compliance examiners are to rely, to the extent possible, on the work conducted by the dedicated supervisory team or primary bank regulator, and expand that analysis to focus on consumer compliance risk. The consumer compliance risk assessment is to include a determination of the level of consumer compliance risk (high, moderate, or low), taking into consideration the internal control and review processes in place to mitigate the inherent risk. In addition, the risk assessment is to include a determination of the direction of consumer compliance risk (increasing, stable, or decreasing). The consumer compliance examiner is to discuss the identified areas of significant consumer compliance risk with the CPC. In addition, in coordination with the CPC and the supervisory team, the consumer compliance examiner is to evaluate how consumer compliance risk affects the reputational, legal, and operational risk profiles of the LCBO or LBO. The CPC will then incorporate this information and the assessment of consumer compliance risk into the LCBO's or LBO's overall risk assessment.

The consumer compliance examiner and the CPC will determine, on a case-by-case basis, whether and what type of supervisory activities should be included in the organization's supervisory plan. The planned supervisory activities will vary depending on the nature and level of an organization's consumer compliance risk.

The CPC and the consumer compliance examiner will coordinate with other regulators before communicating their findings to the banking organization's management. This coordination should help to ensure a seamless process in which consistent messages are delivered to LCBO or LBO management.

10b. The Board's Division of Banking Supervision and Regulation and its Division of Consumer and Community Affairs developed the consumer compliance risk assessment framework. The supervisory approach does not apply to shell BHCs.

2124.01.6.1.3 Adequacy of Information Technology Systems

Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk-monitoring activities must be supported by management information systems (MIS) that provide senior managers and directors with timely and reliable reports on the financial condition, operating performance, and risk exposure of the consolidated organization. Such systems must also provide managers engaged in the day-to-day management of the organization's activities with regular and sufficiently detailed reports for their areas of responsibility. Moreover, in most large complex institutions, MIS not only provides reporting systems but also supports a broad range of business decisions through sophisticated risk-management and decision tools, such as credit scoring and asset/liability models and automated trading systems. Accordingly, the institution's risk assessment must consider the adequacy of information technology systems.

Institutions need to determine which business unit or units are responsible for the development and operation of the information technology system. Traditionally, such systems were largely centered on mainframe computers. However, the development of increasingly powerful and inexpensive personal computers and sophisticated network communication capabilities has given institutions more timely access to a greater volume of information that supports a broader range of business decisions—moving some transaction processing out of the mainframe environment. Consequently, many large institutions are transferring responsibility for development and operation of the hardware (generally, a local area or wide area network) and the related operating systems and applications from a centralized, mainframe function to individual business units. Many of these institutions are also integrating the information technology audit function with the general internal audit function.

Once it has been determined which business units are responsible for information technology, a fuller understanding of the risk profile of specific functions and of the consolidated organization can be gained through close coordination between information systems specialists and safety-and-soundness examiners. Since business managers must have MIS reports that are sufficient and appropriate for identifying risks, examiners must work with specialists to assess the adequacy of the information technology system and the extent to which it can be relied upon. Evaluating the integrity of the information in reports for business managers requires an understanding of the information flows and the control environment for the operation. Knowledge of the business application is essential to determine whether the information flows are complete, accurate, and appropriate in a particular MIS. In addition, such a determination requires an assessment of the extent to which the institution's internal audit function has procedures in place for reviewing and testing the effectiveness of the processes and internal controls related to information technology systems.

2124.01.6.2 Preparation of the Risk Matrix

A risk matrix is used to identify significant activities, the type and level of inherent risks in these activities, and the adequacy of risk management over these activities, as well as to determine composite risk assessments for each of these activities and the overall institution. A risk matrix can be developed for the consolidated organization, for a separate affiliate, or along functional business lines. The matrix is a flexible tool that documents the process followed to assess the overall risk of an institution and is a basis for preparation of the narrative risk assessment.

2124.01.6.2.1 Identification of Significant Activities

Activities and their significance can be identified by reviewing information from the institution, the Reserve Bank, or other supervisors. Information generated by the institution may include the balance sheet, off-balance-sheet reports, the income statement, management accounting reports, or any other report that is prepared for the institution's board of directors and senior management to monitor performance. A detailed income statement is particularly informative because it reflects significant activities and their relative importance to the institution's revenue and net income. The income statement also yields information regarding the relationship between the return on individual assets and the inherent risk associated with these assets, providing an important indicator of the institution's overall risk appetite.

Off-site surveillance information is another source of information that can be used to identify new or expanding business activities. For example, substantial growth in the loan portfolio may indicate that the institution has introduced a new lending activity.

In addition to financial factors, information on strategic plans, new products, and possible management changes needs to be considered. The competitive climate in which the institution operates is important and should be assessed in the identification of significant activities. Industry segmentation and the position the institution occupies within its markets should also be considered.

2124.01.6.2.2 Type and Level of Inherent Risk of Significant Activities

After the significant activities are identified, the type and level of risk inherent in those activities should be determined. Types of risk may be categorized according to section 4070.1.2 and SR-95-51 (as amended by SR-04-18), or by using categories defined either by the institution or other supervisory agencies. If the institution uses risk categories that differ from those defined by the supervisory agencies, the examiner should determine if all relevant types of risk are appropriately captured. If risks are appropriately captured by the institution, the examiner should use the categories identified by the institution.

Table 2 illustrates risk types as defined by the Federal Reserve and the OCC. This table is designed to show the relationship between the respective agencies' risk categories.

Table 2—Types of Risk

Federal Reserve	*OCC*
Credit	Credit
Market	Price Interest rate Foreign exchange
Liquidity	Liquidity
Reputational	Reputation
Operational	Transaction
Legal	Compliance
	Strategic*

* Elements of strategic risk are reflected in each of the risk categories as defined by the Federal Reserve.

For the identified functions or activities, the inherent risk involved in that activity should be described as high, moderate, or low for each type of risk associated with it. For example, it may be determined that a portfolio of commercial loans in a particular institution has high credit risk, moderate market risk, moderate liquidity risk, low operational risk, low legal risk, and low reputational risk. The following definitions apply:

1. *High inherent risk* exists when (1) the activity is significant or positions are large in

relation to the institution's resources or to its peer group, (2) there are a substantial number of transactions, or (3) the nature of the activity is inherently more complex than normal. Thus, the activity could potentially result in a significant and harmful loss to the organization.

2. *Moderate inherent risk* exists when (1) positions are average in relation to the institution's resources or to its peer group, (2) the volume of transactions is average, and (3) the activity is more typical or traditional. Thus, while the activity could potentially result in a loss to the organization, the loss could be absorbed by the organization in the normal course of business.
3. *Low inherent risk* exists when the volume, size, or nature of the activity is such that even if the internal controls have weaknesses, the risk of loss is remote or, if a loss were to occur, it would have little negative impact on the institution's overall financial condition.

It is important to remember that this assessment of risk is made without considering management processes and controls. Those factors are considered in evaluating the adequacy of the institution's risk-management systems.

2124.01.6.2.3 Risk-Management Adequacy Assessment for Significant Activities

When assessing the adequacy of an institution's risk-management systems for identified functions or activities, the CPC or designated staff personnel should place primary consideration on findings related to the following key elements of a sound risk-management system:

1. active board and senior management oversight
2. adequate policies, procedures, and limits
3. adequate risk-management, risk-monitoring, and management information systems
4. comprehensive internal controls

Taking these key elements into account, the contact should assess the relative strength of the risk-management processes and controls for each identified function or activity. Relative strength should be characterized as strong, acceptable, or weak as defined below:

1. *Strong risk management* indicates that management effectively identifies and controls all major types of risk posed by the BHC's activities. Management is fully prepared to address risks emanating from new products and changing market conditions. The board and management are forward looking and active participants in managing risk. Management ensures that appropriate policies and limits exist and are understood, reviewed, and approved by the board. Policies and limits are supported by risk-monitoring procedures, reports, and management information systems that provide management and the board with the information and analysis necessary to make timely and appropriate decisions in response to changing conditions. Risk-management practices and the organization's infrastructure are flexible and highly responsive to changing industry practices and current regulatory guidance. Staff has sufficient experience, expertise, and depth to manage the risks assumed by the institution.

   Internal controls and audit procedures are sufficiently comprehensive and appropriate to the size and activities of the institution. There are few noted exceptions to the institution's established policies and procedures, and none is material. Management effectively and accurately monitors the condition of the institution consistent with the standards of safety and soundness and in accordance with internal and supervisory policies and practices. Risk-management processes are fully effective in identifying, monitoring, and controlling the risks to the institution.
2. *Acceptable risk management* indicates that the institution's management of risk is largely effective but lacking in some modest degree. Management demonstrates a responsiveness and ability to cope successfully with existing and foreseeable risks that may arise in carrying out the institution's business plan. While the institution may have some minor risk-management weaknesses, these problems have been recognized and are in the process of being resolved. Overall, board and senior management oversight, policies and limits, risk-monitoring procedures, reports, and management information systems are considered satisfactory and effective in maintaining a safe and sound institution. Risks are controlled in a manner that does not require more-than-normal supervisory attention.

   The BHC's risk-management practices

and infrastructure are satisfactory and generally are adjusted appropriately in response to changing industry practices and current regulatory guidance. Staff experience, expertise, and depth are generally appropriate to manage the risks assumed by the institution.

Internal controls may display modest weaknesses or deficiencies, but they are correctable in the normal course of business. The examiner may have recommendations for improvement, but the weaknesses noted should not have a significant effect on the safety and soundness of the institution.

3. *Weak risk management* indicates that risk-management practices are lacking in some important ways and, therefore, are a cause for more-than-normal supervisory attention. One or more of the four elements of sound risk management[11] (active board and senior management oversight; adequate policies, procedures, and limits; adequate risk-management monitoring and management information systems; comprehensive internal controls) are considered less than acceptable and have precluded the institution from fully addressing one or more significant risks to its operations. Certain risk-management practices are in need of improvement to ensure that management and the board are able to identify, monitor, and control all significant risks to the institution. Also, the risk-management structure may need to be improved in areas of significant business activity, or staff expertise may not be commensurate with the scope and complexity of business activities. In addition, management's response to changing industry practices and regulatory guidance may need to improve.

   The internal control system may be lacking in some important aspects, particularly as indicated by continued control exceptions or by a failure to adhere to written policies and procedures. The risk-management weaknesses could have adverse effects on the safety and soundness of the institution if corrective action is not taken by management.

The definitions above apply to the risk management of individual functions or activities. They parallel the definitions set forth in section 4070.1.2 (See SR-04-18 and SR-95-51) that examiners are to use to rate an institution's overall risk management. However, unlike the overall risk-management rating, the assessment of the adequacy of risk-management systems incorporated into the risk matrix is to be used primarily for planning supervisory activities. In addition, because the risk matrix is prepared during the planning process, it generally would not be appropriate to make fine gradations in the strength of risk-management systems on a function-by-function basis. In particular, for purposes of rating an institution's overall risk management, section 4070.1.2 (SR-04-18 and SR-95-51) makes distinctions in degrees of weakness—fair, marginal, and unsatisfactory—that generally cannot be made appropriately on a function-by-function basis, as called for when preparing the risk matrix. After appropriate inspection and examination procedures are performed, the assessment of the institution's risk management that was prepared for the risk matrix may be a starting point for assigning an overall risk-management rating for the institution.

2124.01.6.2.4 Composite Risk Assessment of Significant Activities

The composite risk for each significant activity is determined by balancing the overall level of inherent risk of the activity with the overall strength of risk-management systems for that activity. For example, commercial real estate loans usually will be determined to be inherently high risk. However, the probability and the magnitude of possible loss may be reduced by having very conservative underwriting standards, effective credit administration, strong internal loan review, and a good early-warning system. Consequently, after accounting for these mitigating factors, the overall risk profile and level of supervisory concern associated with commercial real estate loans may be moderate. Table 3 provides guidance on assessing the composite risk of an activity by balancing the observed quantity and degree of risk with the perceived strength of related management processes and internal controls.

To facilitate consistency in the preparation of the risk matrix, general definitions of the composite level of risk for significant activities are provided below.

11. See SR-04-18,"Bank Holding Company Rating System," which amended the rating definitions of SR-95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies."

Table 3—Composite Risk for Significant Activities

Risk-management systems	*Inherent risk of the activity*		
	Low	*Moderate*	*High*
	Composite risk assessment		
Weak	Low or moderate	Moderate or high	High
Acceptable	Low	Moderate	High
Strong	Low	Low or moderate	Moderate or high

1. A *high composite risk* generally would be assigned to an activity when the risk-management system does not significantly mitigate the high inherent risk of the activity. Thus, the activity could potentially result in a financial loss that would have a significant negative impact on the organization's overall condition—in some cases, even where the systems are considered strong. For an activity with moderate inherent risk, a risk-management system that has significant weaknesses could result in a high composite risk assessment, because management appears to have an insufficient understanding of the risk and an uncertain capacity to anticipate and respond to changing conditions.
2. A *moderate composite risk* generally would be assigned to an activity with moderate inherent risk where the risk-management systems appropriately mitigate the risk. For an activity with a low inherent risk, significant weaknesses in the risk-management system may result in a moderate composite risk assessment. On the other hand, a strong risk-management system may reduce the risks of an inherently high-risk activity so that any potential financial loss from the activity would have only a moderate negative impact on the financial condition of the organization.
3. A *low composite risk* generally would be assigned to an activity that has low inherent risks. An activity with moderate inherent risk may be assessed a low composite risk where internal controls and risk-management systems are strong and effectively mitigate much of the risk.

2124.01.6.2.5 Overall Composite Risk Assessment

Once the examiner has assessed the composite risk of each identified significant activity or function, an overall composite risk assessment should be made for off-site analytical and planning purposes. This assessment is the final step in the development of the risk matrix; the evaluation of the overall composite risk is incorporated into the written risk assessment.

2124.01.6.2.6 Preparation of the Risk Assessment

A written risk assessment should be prepared to serve as an internal supervisory planning tool and to facilitate communication with other supervisors. A sample risk assessment is provided below. The goal is to develop a document that presents a comprehensive risk-focused view of the institution. The risk assessment delineates the areas of supervisory concern and is a platform for developing the supervisory plan.

The format and content of the written risk assessment are flexible and should be tailored to the individual institution. The risk assessment reflects the dynamics of the institution and, therefore, should consider the institution's evolving business strategies and be amended as significant changes in the risk profile occur. It should include input from other affected supervisors and specialty units to ensure that all significant risks of the institution are identified. The risk assessment should—

1. include an overall risk assessment of the organization;
2. describe the types of risks (credit, market, liquidity, reputational, operational, legal), their level (high, moderate, low), and the direction (increasing, stable, decreasing) of risks;
3. identify all major functions, business lines, activities, products, and legal entities from which significant risks emanate, and identify the key issues that could affect the risk profile;
4. consider the relationship between the likelihood of an adverse event and the potential impact on an institution (for example, the likelihood of a computer system failure may be remote, but the financial impact could be significant); and
5. describe the institution's risk-management systems. Reviews and risk assessments performed by internal and external auditors

should be discussed, as should the ability of the institution to take on and manage risk prospectively.

The CPC should attempt to identify and report the cause of unfavorable trends, as well as their symptoms. Also, it is very important that the risk assessment reflect a thorough, detailed analysis that supports the conclusions made about the institution's risk profile.

2124.01.7 PLANNING AND SCHEDULING SUPERVISORY ACTIVITIES

The supervisory plan is a bridge between the institution's risk assessment, which identifies significant risks and supervisory concerns, and the supervisory activities to be conducted. In developing the supervisory plan and inspection and examination schedules, the CPC should minimize disruption to the institution and, whenever possible, avoid duplicative inspection and examination efforts and requests for information from other supervisors.[12]

The institution's organizational structure and complexity are significant considerations in planning the specific supervisory activities to be conducted. Additionally, interstate banking and branching activities have implications for planning on-site and off-site reviews. The scope and location of on-site work for interstate banking operations will depend on the significance and risk profile of local operations, the location of the supervised entity's major functions, and the degree of its centralization. Consistent with the Federal Reserve practice of not examining each branch of an intrastate branching network, the bulk of safety-and-soundness examinations for branches of an interstate bank would likely be conducted at the head office or regional offices, supplemented by periodic reviews of branch operations and internal controls. The supervisory plan should reflect the need to coordinate these reviews of branch operations with other supervisors.

2124.01.7.1 Preparation of the Supervisory Plan

A comprehensive supervisory plan should be developed annually and updated as appropriate for the consolidated organization.[13] The plan should demonstrate the supervisory concerns identified through the risk-assessment process and how the deficiencies noted in the previous inspection or examination are being or will be addressed. To the extent that the institution's risk-management systems are adequate, the level of supervisory activity may be adjusted. The plan should generally address the following areas:

1. All supervisory activities to be conducted, the scope of those activities (full or targeted), the objectives of those activities (for example, review of specific business lines, products, support functions, legal entities), and specific concerns regarding those activities, if any. Consideration should be given to—
   a. prioritizing supervisory resources on areas of higher risk,
   b. pooling examiner resources to reduce burden and redundancies,
   c. maximizing the use of examiners located where the activity is being conducted,
   d. coordinating examinations of different disciplines,
   e. determining compliance with or the potential for supervisory action, and
   f. balancing mandated requirements with the objectives of the plan.
2. General logistical information (for example, timetable of supervisory activities, participants, and expected resource requirements).
3. The extent to which internal and external audit, internal loan review, compliance, and other risk-management systems will be tested and relied upon.

The planning horizon to be covered by the plan is generally 18 months for domestic institutions.[14] The overall supervisory objectives and basic framework need to be outlined by midyear

12. See section 5000.0.8.3 and SR-93-30, "Interagency Policy Statements on Supervisory Initiatives," and its attachments for guidance on examination coordination of holding company inspections with subsidiary bank and thrift examinations. See SR-00-14, "Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign Banking Organizations," regarding coordination with other agencies as part of the FBO supervision program.

13. The supervisory plan is a high-level plan of supervisory activities to be conducted in monitoring the consolidated organization. More-detailed procedures for a specific on-site inspection are appropriately addressed in a scope memorandum, which is discussed in section 2124.01.8.

14. The examination plans and assessments of condition of U.S. operations that are used for FBO supervision use a 12-month period.

to facilitate preliminary discussions with other supervisors and to coincide with planning for the Federal Reserve's scheduling conferences. The plan should be finalized by the end of the year, for execution in the following year.

2124.01.7.2 Preparation of the Inspection or Examination Program

The inspection or examination program should provide a comprehensive schedule of inspection or examination activities for the entire organization and aid in the coordination and communication of responsibilities for supervisory activities. An inspection or examination program provides a comprehensive listing of all inspection and examination activities to be conducted at an institution for the given planning horizon. To prepare a complete program and to reflect the current conditions and activities of an institution and the activities of other supervisors, the CPC needs to be the focal point for communications on a particular institution, including any communications with the Federal Reserve and the institution's management and other supervisors. The inspection or examination program should generally incorporate the following logistical elements:

1. a schedule of activities, the duration of time, and resource estimates for planned projects
2. an identification of the agencies conducting and participating in the supervisory activity (when conducted jointly with other agencies, indicate the lead agency and the agency responsible for a particular activity) and the resources committed by all participants to the area(s) under review
3. the planned product for communicating findings (indicate whether it will be a formal report or supervisory memorandum)
4. the need for special examiner skills and the extent of participation by specialty disciplines

2124.01.8 DEFINING INSPECTION OR EXAMINATION ACTIVITIES

The scope memorandum is an integral product in the risk-focused methodology. The memorandum identifies the key objectives of the on-site inspection or examination. The focus of on-site inspection or examination activities, as identified in the scope memorandum, should be oriented to a top-down approach that includes a review of the organization's internal risk-management systems and an appropriate level of transaction testing. The risk-focused methodology provides flexibility in the amount of on-site transaction testing. Although the focus of the inspection or examination is on the institution's processes, an appropriate level of transaction testing and asset review will be necessary to verify the integrity of internal systems. If internal systems are considered reliable, then transaction testing should be targeted to a level sufficient to validate that the systems are effective and accurate. Conversely, if internal management systems are deemed unreliable or ineffective, then transaction testing must be adjusted to increase the amount of coverage. The entry letter identifies the information necessary for the successful execution of the on-site inspection or examination procedures.

2124.01.8.1 Scope Memorandum

After the areas to be reviewed have been identified in the supervisory plan, a scope memorandum should be prepared that documents specific objectives for the projected inspection or examination. This document is of key importance, as the scope will likely vary from year to year. Thus, it is necessary to identify the specific areas chosen for review and the extent of those reviews. The scope memorandum will help ensure that the supervisory plan for the institution is executed, and it will define and communicate those specific objectives to the inspection or examination staff.

The scope memorandum should be tailored to the size, complexity, and current rating of the institution subject to review. For large but less-complex institutions, the scope memorandum may be combined with the supervisory plan or risk assessment. The scope memorandum should generally include—

1. a statement of the objectives;
2. an overview of the activities and risks to be evaluated;
3. the level of reliance on internal risk-management systems and internal or external audit findings;
4. a description of the procedures that are to be performed, indicating any sampling process to be used and the level of transaction testing, when appropriate;
5. identification of the procedures that are expected to be performed off-site; and

6. a description of how the findings of targeted reviews, if any, will be used on the current inspection or examination.

2124.01.8.2 Entry Letter

Standardized entry inspection and examination letters have been developed that are closely aligned with the risk-focused approach for large complex institutions.[15] The letters are designed to reduce the institution's paperwork burden. The entry letters include a core section of required information that is pertinent to all large institutions, regardless of size or complexity. In addition to the core requests, supplementary questionnaires should be used as needed for the specialized areas such as asset securitization/sales, information systems, private banking, securities clearance/lending, trading activities, and transfer risk. The cover letters must be used (but can be modified), as they provide specific guidance to the inspected or examined institution.

The entry letters direct management to provide written responses to questions and to provide copies of specific documents requested, but only if the requested information is new or has changed since the previous examination or inspection. Examiners should not request that management provide them with copies of the institution's regulatory reports that are available within each Federal Reserve Bank or from other bank regulatory agencies, such as regulatory inspection and examination reports and various financial information (for example, annual reports or Call Reports). These reports should be gathered from internal sources during the pre-examination planning process. Also, entry letters should not request information that is regularly provided to designated CPCs. The examiner-in-charge should always review anticipated information and document needs with the CPC for the inspected or examined institution before the mailing of any entry letter.

The entry letters should be used as a starting point, or template, in preparing for an examination or inspection. They should be tailored during the planning process to fit the specific character and profile of the institution to be inspected or examined and the scope of the activities to be performed. Thus, the effective use of entry letters is highly dependent on the planning and scoping of a risk-focused inspection or examination.

The entry letters request internal management information reports for each of the key inspection or examination areas. Internal management reports should be used in all instances. If they do not provide sufficient information to inspect or examine the institution, then it would appear that management is not adequately informed—this may well be the first inspection or examination finding. As specific items are selected for inclusion in the entry letter, the following guidelines for items should be considered:

1. *Reflect risk-focused supervision objectives and the inspection or examination scope.* Items that are not needed to support selected inspection or examination procedures should not be requested.
2. *Facilitate efficiency in the inspection or examination process and lessen the burden on financial institutions.* Minimize the number of requested items and avoid, to the extent possible, duplicate requests for information already provided to other agencies.
3. *Limit, to the extent possible, requests for special management reports.*
4. *Eliminate items used for audit-type procedures.* Such procedures (for example, verifications) are generally performed only when there is a reason to suspect that significant problems exist.
5. *Distinguish information to be mailed to the examiner-in-charge for off-site inspection or examination procedures from information to be held at the institution for on-site procedures.* Information that is not easily reproduced should be reviewed on-site (for example, policies, corporate minutes, or audit workpapers).
6. *Allow management sufficient lead time to prepare the requested information.*

2124.01.9 PERFORMING INSPECTION OR EXAMINATION PROCEDURES

Inspection or examination procedures should be tailored to the characteristics of each institution, keeping in mind its size, complexity, and risk profile. The procedures should focus on developing appropriate documentation to adequately assess management's ability to identify, measure, monitor, and control risks. Procedures should be completed to the degree necessary to determine whether the institution's management understands and adequately controls the levels and types of risks that are assumed. In terms of

15. Such entry letters should be used for a (1) combined bank holding company inspection and lead state member bank examination, (2) bank holding company inspection (see appendix B), and (3) state member bank examination.

transaction testing, the volume of transactions tested should be adjusted according to management's ability to accurately identify problem and potential problem transactions and to measure, monitor, and control the institution's risk exposure. Likewise, the level of transaction testing for compliance with laws, regulations, and supervisory policy statements should take into account the effectiveness of management systems to monitor, evaluate, and ensure compliance.

Most full-scope inspections or examinations are expected to include the examiners' evaluation of 10 functional areas during the supervisory cycle. There may be a need to identify and include additional functional areas. To evaluate these functional areas, examiners must perform procedures tailored to fit (1) the risk assessment prepared for the institution and (2) the scope memorandum. These functional areas represent the primary business activities and functions of large complex institutions, as well as common sources of significant risk to them. Further, consistent with the risk-focused approach, examiners are expected to evaluate other areas that are significant sources of risk to an institution or that are central to the assignment of CAMELS, RFI/C(D), and ROCA ratings. The identified functional areas include the following:

1. loan-portfolio analysis (portfolio management, loan review, consumer compliance, allowance for loan and lease losses)
2. treasury activities (asset-liability management, interest-rate risk, parent company liquidity, funding, investments, deposits)
3. trading and capital-markets activities (foreign exchange, commodities, equities, and other interest-rate risk; credit risk; and liquidity risk)
4. audit and internal control review
5. final assessment of supervisory ratings (CAMELS, RFI/C(D), ROCA, or other)
6. information systems
7. insurance and fiduciary activities
8. private banking
9. retail banking activities (new products and delivery systems)
10. payments system risk (wire transfers, reserves, settlement)

2124.01.10 REPORTING THE FINDINGS

After performing the inspection or examination procedures, examiners should document their overall conclusions. Conclusions, as they relate to the functional area under review, should clearly communicate the examiner's assessment of the internal risk-management system, the financial condition, and compliance with laws and regulations.

Inspection and examination activities should be coordinated with the respective state and other federal banking authorities, with joint examinations performed and joint inspection and examination reports completed wherever practicable. The inspection and examination activities should be planned over the supervisory cycle, culminating with an annual full-scope inspection or examination of the organization. As part of the FBO supervision program, individual examination findings are integrated into an assessment of the FBO's entire U.S. operations.

The results of a targeted, subsidiary, or specialty inspection or examination are usually reported to the institution's management in a separate report or supervisory letter. Therefore, the report for the annual full-scope inspection of the consolidated parent organization should include a summary of the relevant results of any preceding supervisory activity. When targeted or specialty inspections or examinations of affiliates are conducted concurrently with the annual full-scope inspection of the consolidated parent organization, the findings from the targeted, consumer compliance, or specialty examinations (fiduciary, insurance, information technology, etc.) should be incorporated into the parent's inspection report in lieu of separate reports, unless the institution's management requests separate reports. For organizations in which the lead bank is a state member bank, the annual full-scope examination report should be combined with the bank holding company inspection report, as appropriate. The bank holding company inspection report, or combined inspection/examination report, may also include other bank and nonbank subsidiary examinations, according to the organization's supervisory plan.

The contents of the report should clearly and concisely communicate to the institution's management or to the directorate any supervisory issues, problems, or concerns related to the institution, as well as disclose the assigned

supervisory rating.[16] The report should also include appropriate comments regarding deficiencies noted in the institution's risk-management systems. Accordingly, the descriptions accompanying each component of the CAMELS rating system should emphasize management's ability to identify, measure, monitor, and control risks.[17] The rating assigned should reflect the adequacy of the institution's risk-management systems in light of the amount and types of risks that the institution has taken on.

16. See section 5010.4 and SR-96-26 for additional information.

17. See SR-96-38 for additional information on the revised CAMELS rating system.

2124.01.11 APPENDIX A—RISK-FOCUSED SUPERVISORY LETTERS AND BHC SUPERVISION MANUAL SECTION NUMBERS

SR-letter	*SR-letter title*	*BHCSM section no.*
SR-08-9/ CA-08-12	Consolidated Supervision of Bank Holding Companies and the Combined U.S. Operations of Foreign Banking Organizations	1050.0
SR-08-8/ CA-08-12	Compliance Risk-Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles	2124.08
SR-06-15/ CA-06-12	Interagency Guidance on Nontraditional Mortgage Product Risks	3070.3
SR-05-11	Interagency Credit Risk-Management Guidance for Home Equity Lending	2010.2
SR-04-18	Bank Holding Company Rating System (Revised)	4070.0
SR-03-22	Framework for Assessing Consumer Compliance Risk at Bank Holding Companies	2124.01.6.1.2
SR-03-5	Interagency Policy Statement on the Internal Audit Function and Its Outsourcing	2060.05.06
SR-03-4	Risk Management and Valuation of Mortgage Servicing Assets Arising from Mortgage Banking Activities	3070.0
SR-02-20	The Sarbanes-Oxley Act of 2002	2060.05
SR-02-5	Interagency Guidance on Country Risk Management	4090.0
SR-02-1	Revisions to Bank Holding Company Supervision Procedures for Organizations with Total Consolidated Assets of $5 Billion or Less	5000.0.4.3
SR-00-17	Guidance on the Risk Management of Outsourced Technology Services	2124.1
SR-00-14	Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign Banking Organizations	2124.0
SR-00-13	Framework for Financial Holding Company Supervision	3900.0
SR-99-37	Risk Management and Valuation of Retained Interests Arising from Securitization Activities	2128.06
SR-99-23	Recent Trends in Bank Lending Standards for Commercial Loans	2010.2.2 2010.10
SR-99-18	Assessing Capital Adequacy in Relation to Risk at Large Banking Organizations and Others with Complex Risk Profiles	4060.7
SR-99-17	Supervisory Ratings for State Member Banks, Bank Holding Companies, and Foreign Banking Organizations, and Related Requirements for the National Examination Data System	

SR-letter	*SR-letter title*	*BHCSM section no.*
SR-99-15	Risk-Focused Supervision of Large Complex Banking Organizations	2124.04
SR-99-6	Subprime Lending	2128.08
SR-99-3	Supervisory Guidance Regarding Counterparty Credit Risk Management	2126.3
SR-98-18	Lending Standards for Commercial Loans	2122.0
SR-98-12	FFIEC Policy Statement on Investment Securities and End-User Derivatives Activities	2126.1
SR-98-9	Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations	2124.1
SR-97-24	Risk-Focused Framework for Supervision of Large Complex Institutions	2124.01
SR-97-21	Risk Management and Capital Adequacy of Exposures Arising from Secondary Market Credit Activities	2129.05
SR-96-38	Uniform Financial Institution Rating System (CAMELS—adding the "S" for risk management)	4020.9, 4070.0.4, 4080.0
SR-96-33	State/Federal Protocol and Nationwide Supervisory Agreement	
SR-96-29	Supervisory Program for Risk-Based Inspection of Top 50 Bank Holding Companies	
SR-96-27	Guidance on Addressing Internal Control Weaknesses in U.S. Branches and Agencies of Foreign Banking Organizations Through Special Audit Procedures	
SR-96-26	Provisions of Individual Components of the Rating System	5010.4
SR-96-17	Supervisory Guidance for Credit Derivatives	2129.0
SR-96-14	Risk-Focused Safety and Soundness Examinations and Inspections	2124.0
SR-96-13	Joint Policy Statement on Interest-Rate Risk	2127.0
SR-96-10	Risk-Focused Fiduciary Examinations	
SR-95-51	Rating the Adequacy of Risk Management and Internal Controls at State Member Banks and Bank Holding Companies	4070.1
SR-93-69	Examining Risk Management and Internal Controls for Trading Activities of Banking Organizations	2125.0
SR-93-19	Supplemental Guidance for Inspection of Nonbank Subsidiaries of Bank Holding Companies	5000.0.4.4

2124.01.12 APPENDIX B—NONBANK SUBSIDIARY RISK-ASSESSMENT QUESTIONNAIRE

NONBANK SUBSIDIARY OF A BANK HOLDING COMPANY RISK-ASSESSMENT QUESTIONNAIRE

Name of subsidiary _____

Name of bank holding company _____

BHC Consolidated:
Tier 1 capital: $_____ Total operating revenue*: $_____

*Defined as the sum of total interest income and total non-interest income, before extraordinary items.

Subsidiary total assets: $_____ Subsidiary total operating revenue: $_____

Questions: *(Circle answer.)*

1. Are the subsidiary's total assets 10 percent or more of BHC consolidated tier 1 capital? Yes No

2. Is the subsidiary's total operating revenue 10 percent or more of BHC consolidated operating revenue? Yes No

3. Does the subsidiary issue debt to unaffiliated parties? Yes No

4. Does the subsidiary rely on affiliated banks for funding debt that is either greater than $10 million or 5 percent of BHC consolidated tier 1 capital? (See SR-93-19.) Yes No

5. Is the subsidiary involved in asset securitization? Yes No

6. Does the subsidiary generate assets and sell assets to affiliates? Yes No

7. Is the subsidiary a broker-dealer affiliate engaged in underwriting, dealing, or market making? Yes No

8. Does the subsidiary provide derivative instruments for sale or as a service to unaffiliated parties? Yes No

9. Has the subsidiary had a significant impact on the BHC's condition or performance? Yes No

If any question is answered yes, then this subsidiary should be considered for on-site review. If an on-site review is not being conducted, state the reason below.

Prepared by: _____ Date: _____

2124.01.13 APPENDIX C—FEDERAL RESERVE BANK COVER LETTER AND BHC INSPECTION QUESTIONNAIRE

Federal Reserve Bank
of San Francisco

Division of Banking Supervision and Regulation
San Francisco, California 94120

D.F. Roe
Senior Vice President
DEF BanCorp
Greentree Boulevard
Anytown, U.S.A. 11111

Dear Mr. Roe:

In order to facilitate an inspection of DEF BanCorp on a fully consolidated basis, you are requested to instruct the appropriate staff to provide the information described in this questionnaire. Unless indicated otherwise, information is requested as of the financial statement date December 31, 20X2. You are asked to provide written responses to questions and copies of specific documents requested in this questionnaire only if the requested information is new or has changed since the previous inspection, which was conducted as of December 31, 20X1 (indicate no change where applicable). For each area covered by this questionnaire, please provide the most recent reports used by management to identify, measure, monitor, and control risk in the respective areas. Please note that examiners may make additional requests during the inspection.

Single copies of all submissions in response to the requests will be satisfactory unless otherwise indicated and should be delivered to the examiner-in-charge or designee. Any requests for clarification or definition of terms should also be directed to the examiner-in-charge.

In order to expedite the inspection, each completed schedule and other requested information should be submitted as soon as prepared and should not be accumulated for submission as a package. Please respond to every item in the questionnaire, indicating N/A if a question is not applicable.

Most of the requested data will not be needed until the commencement of the inspection, which is March 15, 20X3. However, certain information may be needed earlier. Such information and the date due will be discussed with you.

Federal Reserve examiner-in-charge _____ Examiner's telephone number _____

FEDERAL RESERVE BANK
BANK HOLDING COMPANY INSPECTION QUESTIONNAIRE

Please provide the following:

Structure

1. The most recent organization chart—
   (a) for the holding company and its subsidiaries by legal entity, showing percentage of ownership if less than 100 percent; and
   (b) of management by legal entity and functional business lines, if different, indicating lines of authority and allocation of duties for all key business lines and support areas of the organization.
2. List new activities that the bank holding company or nonbank subsidiaries have engaged in since the previous inspection, either on- or off-balance-sheet, and identify the group responsible for the management of these activities. How has management identified and evaluated risk in relation to these new activities? Provide copies of any management reports regarding these products/activities. Please provide a copy of the company's risk policy statement regarding new activities.
3. The following on each new subsidiary formed or acquired since the prior inspection and changes, where applicable, on existing subsidiaries.
   (a) name
   (b) location
   (c) date acquired or formed
   (d) percentage of ownership
   (e) nature of business or business purpose
   (f) list of branch locations by city and state
   (g) balance sheet and income statement
   (h) off-balance-sheet, asset securitization, and derivatives activities and description of such
   (i) list of principal officers
   (j) management contact person
4. Since (date), has there been any change in or transfer of functions or responsibilities between the corporation and its subsidiaries and between subsidiaries and/or their affiliates? If so, describe fully.
5. Since (date), have there been any sales or other transfers of any assets among the corporation and its subsidiary banks, affiliates of the banks, and/or other subsidiaries? If so, describe fully and include details on loan participations purchased and sold.
6. Since (date), have any subsidiaries been deactivated, sold, liquidated, transferred, or disposed of in some other way? If so, identify the subsidiary, the reason for disposition, and the effective date of disposition.
7. Has the corporation planned or entered into any new agreements, written or oral, to acquire any additional entities? If so, give pertinent details, including name, location, type of business, and purchase terms.

Corporate Planning and Policy Information

8. The latest financial projections or business plan(s) for revenues, expenses, assets, liabilities, capital, and contingent liabilities for the current and next fiscal years. Please include details on the assumptions used in the preparation of the projections.
9. A copy of the strategic business plan with updates or revisions, if any.
10. If new or amended since the prior inspection, copies of policies for the following:
    (a) the level of supervision exercised over subsidiaries
    (b) loans and investments of subsidiaries
    (c) loan participations by and between subsidiaries
    (d) dividends and fees from subsidiaries
    (e) dividends paid to stockholders
    (f) budgeting and tax planning for subsidiaries
    (g) insider transactions
    (h) funds, asset-liability, and interest-rate risk management at the parent company and subsidiaries
    (i) risk identification, evaluation, and control (for example, any credit risks, market risks, liquidity risks, reputational risks, operational risks, and legal risks)
    (j) internal loan-review and -grading system
    (k) internal audit
    (*l*) any authorized outstanding commitments to the Federal Reserve
    (m) description of any routine tie-in arrangements that are used in providing or contracting for services

Corporate Financial Information

11. For the consolidated company, provide consolidating balance sheet and income statement, including schedules of eliminating entries.
12. Full details on unaffiliated borrowings of the consolidated organization. For debt issued since the prior inspection, please provide the prospectus for public-debt offerings and a summary of terms for private-debt placements.
13. A copy of the most current periodic financial package prepared for senior management and/or directors.

Subsidiary Information

14. Consolidating and consolidated balance sheets, including off-balance-sheet items, and income statements for each nonbank first-tier subsidiary.
15. Details of all capital injections made to subsidiaries or returns of capital from subsidiaries (excluding normal operating dividends) since the prior inspection. Also provide details on any advance to a subsidiary which has been reclassified as equity.
16. If subsidiary banks have made any extensions of credit to the bank holding company and/or other affiliates, give details.

17. Describe any services performed by the parent for any subsidiaries or any company in which it has a 5 percent or greater interest.

Parent Company

18. Details on intercompany payments either (1) from the parent company to affiliates or subsidiaries or (2) from subsidiaries or affiliates to the parent company. Segregate into dividends, interest, management or service fees, expense payments, or other transfers made since the prior inspection. If a payment is governed by an intercompany agreement, please provide a copy of the agreement. If not, please provide the basis of the payment made.
19. Internally generated cash-flow statement and liquidity schedule for the latest quarter ending. Make available supporting documentation. Provide access to the workpapers supporting the preparation of the Cash-Flow Schedule (schedule PI-A) from the Y-9LP report
20. Full details on new parent company's investments in or advances to subsidiaries, and extensions of credit to and borrowings from subsidiaries (including unused lines of credit) since the previous inspection.
21. Full details on the terms of any third-party borrowing and credit lines made available since the previous inspection.
22. If any entities (parent company and/or subsidiaries) maintain compensating balances with third parties, indicate restrictions, if any.
23. A copy of the contingency funding plan. If such a plan does not exist, please provide a description of what actions would be taken to meet disruptions in the corporation's short-term liability market.
24. Details on security and other investments held by type; par; book and market values; number of shares owned; interest rates; maturity dates; and convertibility features, where applicable. Include a copy of all investment authorization policies and delegations of authority pertaining thereto.
25. For equity investments or any lending activity, please provide a listing with comments on any significant items that may not be fully collectible and any other relevant factors.
26. A copy of the capital funding plan or planned changes in equity funding, a financial analysis of any changes in equity (including any stock redemptions), and any internal financial analysis used to evaluate capital adequacy.
27. Since the previous inspection, if the corporation has purchased or sold securities or other assets under an agreement to resell or repurchase, give details.
28. If the corporation has, for its own account, any incomplete purchases or sales of securities pending, give details.
29. If the parent corporation and/or any nonbank subsidiaries have loans outstanding that are secured by stock or any obligations of the corporation or any of its subsidiaries, give details.
30. Since the prior inspection, if the corporation, either for its own account or for others, has guaranteed the payment of any loan or other debt obligation or guaranteed the performance of any other undertaking, provide details.

Corporate-Debt-Markets Activities

31. The following information on commercial paper:
    (a) direct placements outstanding

(b) dealer placements outstanding

(c) monthly maturity schedules showing breakdown for direct and dealer placements

(d) a copy of a ''no action'' letter, if the SEC has issued one

32. Identify any subsidiary which sells commercial paper for its own use or for its parent.

33. If any commercial paper, stock, and/or convertible debt of the corporation or its subsidiaries is held by trust departments of subsidiary banks, provide details.

34. If there are any concentrations of commercial paper holdings in excess of 10 percent of the outstanding commercial paper by any individual or organization, provide details.

Corporate Tax Information

35. If the corporation files a consolidated tax return, on what basis does it determine the amount of taxes to be paid by subsidiaries? Provide a copy of the tax-sharing agreement with subsidiaries.

36. A schedule detailing the following information for (specify dates)—

(a) payments (estimated or otherwise) made by the corporate-tax-paying entity to the taxing authorities and the dates of such payments; and

(b) payments received by the tax-paying entity from other holding company subsidiaries (or the tax benefits paid to those subsidiaries) and transaction dates.

37. Provide details of any ongoing IRS audit.

Officers, Directors, and Shareholders

38. For senior officers of the corporation, indicate their title, responsibility, and position(s) held at subsidiary and/or other organizations.

39. List of directors of the corporation, including—

(a) number of shares owned directly and/or indirectly, and

(b) occupation or principal business affiliation.

40. A brief biography of each senior officer appointed and director elected since the prior inspection. Please include the person's date of birth, business background, education, and affiliations with any outside organizations. For senior officers, indicate date of hire. For directors, indicate date of election to board.

41. List of board committees, their memberships, and frequency of meetings.

42. Make available board and committee minutes.

43. Details on fees paid to directors.

44. If the corporation has entered into any contracts or agreements to pay or provide additional sums or fringe benefits to any director, officer, or employee, provide cost and details.

45. Details on any stock option, incentive, bonus, or performance plans for officers and employees.

46. List of loans made by the parent company and/or nonbank subsidiaries to directors and executive officers (and their interests) of the parent company and/or subsidiaries. For the purpose of this request, a director's or executive officer's interest refers to a beneficial ownership, directly or indirectly, amounting to 25 percent or more and also to companies otherwise controlled by a director or officer.

47. List of investments of the parent and/or subsidiaries in stocks, bonds, or other obligations of

corporations in which directors and executive officers have a beneficial interest.

48. List of loans to any borrower that are secured by stocks, bonds, or other obligations of corporations in which directors and executive officers have a beneficial interest.

49. List of shareholders who own 5 percent or more of any class of voting stock and the percentage held.

50. List of loans made by the parent company and/or nonbank subsidiaries to shareholders who own 5 percent or more of the parent company's outstanding shares.

Asset Quality

51. A copy of the latest internal consolidated asset-quality tracking report with aggregate totals of internally criticized assets and off-balance-sheet items. Identify aggregate exposures by type, risk rating, and entity where the exposure is booked. Distinguish between direct and indirect extensions of credit.

52. Details on consolidated loans past due as to principal and/or interest, nonperforming loans and other real estate owned, and totals of such for each subsidiary.

53. A breakdown of the corporation's consolidated and major subsidiaries' loan-loss reserves (for example, the allowance for loan and lease losses), including portions earmarked for the commercial, consumer, and other segments, with a description of and supporting data for the methodology used in determining its adequacy.

Audit

(The following information should be requested only if the function resides within the parent company. If the function is performed at a nonmember lead bank subsidiary, then assess the audit function through discussions with the bank's primary regulator.)

54. A copy of the most recent engagement letters or equivalent information which describes the scope of external audit activities performed for the corporation and any of its nonbank subsidiaries. Make available a copy of the audit program.

55. An organization chart which shows the structure and staffing of the audit function.

56. The following information about the auditor and key assistants (if not provided at prior inspections):

    (a) present position and date assumed

    (b) date of employment

    (c) brief summary of education, experience at this institution, and prior work experience

57. Make available the audit timetable and audit program, workpapers, and procedures used in conducting audits of the parent company and all subsidiaries.

Miscellaneous

58. A summary schedule of fidelity bond and general liability insurance, listing all areas covered for loss/liability, and date of board approval.

59. Make available the corporation's latest pending litigation report describing any significant pending or potential litigation or investigations against the organization or any director, officer, or policy-making employee in their official capacity, with the following information:

(a) name(s) of plaintiff

(b) nature of claim and damages requested

(c) current status

(d) an opinion of the probable outcome, including an estimation of the organization's liability

The Federal Reserve's ongoing large complex banking organization (LCBO) supervisory program is designed to recognize dramatic changes in the financial, technological, legal, and regulatory environment that necessitate a flexible supervisory framework. This includes the ongoing review and assessment of LCBO risk profiles and the continual adjustment of supervisory plans and programs for individual banking organizations (BOs). Environmental factors that have a significant impact on the nature of LCBO operations and the financial system include the following:

1. *Financial innovation and deregulation.* The range, volume, and complexity of traditional banking businesses have increased, and BOs have moved into nontraditional and potentially more-complex financial activities and services, such as securitizations, securities underwriting and dealing, trading, derivatives, and other capital-markets activities.[1]
2. *Increasing competitive pressures.* The distinctions between financial products have blurred, and the competition in national and global markets between BOs, nonbank financial firms, and diversified financial services conglomerates has intensified.
3. *Geographic expansion and globalization.* The continued expansion of BOs, both nationally and globally, and the integration of financial markets have increased the challenges associated with assessing and supervising the worldwide activities of U.S. BOs and the U.S. operations of foreign banking organizations.
4. *Revolution in information technology.* The dramatic changes in information and telecommunications technology have increased the speed, complexity, geographic scope, and volume of financial transactions, and have made possible new techniques for BOs to take on and manage risks.

These environmental factors have the potential for swift and dramatic changes in the risk profiles of LCBOs and can provide avenues for the more rapid transmission of financial shocks. Such developments in turn require supervisors to employ more-continuous and risk-focused supervision processes. See SR-99-15, SR-97-24, and section 2124.01.

2124.04.1 CONTINUED UNDERSTANDING OF AN LCBO AND ITS MAJOR RISKS

The process of maintaining a *current* understanding of an LCBO and its major risks relies heavily on gathering information from a wide variety of public and confidential sources, including supervisory reviews and evaluations and discussions with management and other supervisors. One of the primary objectives of this enhanced supervisory method is to generate a flow of meaningful information that continuously promotes a comprehensive understanding of the LCBO. This understanding should include the LCBO's major business lines and strategies, the risks inherent in its business activities, and the quality and effectiveness of its risk-management systems. Maintaining an up-to-date understanding of an LCBO's risk profile reduces the time-consuming and burdensome discovery process associated with conducting on-site examinations. Similarly, this understanding can also facilitate the timely and efficient processing of major regulatory applications, including acquisitions and mergers, and other requests from BOs. Publicly available information, internal management reports, discussions with management, regulatory reports, information from internal and external auditors, and information from other supervisors are examples of the sources that are used to develop and maintain a current understanding of the organization. It may be less burdensome for the BO if supervisors can access management reports electronically, so electronic access should be employed when and where feasible and appropriate.

It is important that the principal risk-focused supervisory tools and documents, including the overview, risk matrix, and risk assessment for the LCBO, remain current. Accordingly, the central point of contact (CPC) should regularly distill and incorporate significant new information into these documents *at least quarterly.* Factors such as emerging risks; new products; and significant changes in business strategy, management, condition, or ownership may warrant more-frequent updates. In general, the more dynamic the LCBO's operations and risks, the more frequently the CPC should update the risk assessment, strategies, and plans.

1. The term "banking organizations" refers to bank holding companies and their bank and nonbank subsidiaries.

2124.04.2 DESIGN AND EXECUTION OF A CURRENT SUPERVISORY PLAN

Effective risk-focused supervision requires the development and maintenance of a supervisory plan that is current and relevant to the organization's changing risk profile. In addition to addressing all key supervisory objectives, the supervisory plan should be individually tailored for each BO to reflect its particular organizational and operational structure and, where appropriate, the activities of other principal or functional supervisors. The supervisory plan and attendant supervisory activities, including on-site examinations, inspections, and supervisory reviews, should be sufficiently robust to maintain an up-to-date and thorough understanding of the BO's operations and risks, as well as to maintain the quality of its risk-management systems.

Ongoing assessments of the LCBO's major risks (for example, credit, market, liquidity, operational, legal, and reputational risks) should be used to formulate, revise, and update the supervisory plan. The Federal Reserve's supervisory plan should endeavor to take into account (1) the nature and scope of major activities conducted by other regulators involved in the LCBO and (2) any actions necessary to address existing or emerging supervisory concerns, including follow-up on past supervisory issues. For BOs supervised by the Federal Reserve, a combination of full- and limited-scope examinations, inspections, targeted reviews, meetings with management, and analyses of public and supervisory information should be used to maintain an up-to-date risk assessment and to reduce unnecessary regulatory burden. The necessary level of transaction testing and the degree of reliance on sampling should be fully explained in the scope documents of the supervisory plan and should adequately address the types and level of risks in the organization's business lines. Instances in which efficiencies can be gained by relying on the work of other regulators, internal and external auditors, and the internal risk-management function should, where appropriate, be specified in the plan and incorporated into the supervisory program.

The CPC should review and revise the supervisory plan whenever necessary *(but in no case less frequently than quarterly)* to reflect any significant new information or emerging trends or risks. The supervisory plan and any revisions should be periodically discussed with representatives of the principal regulators of major affiliates to reconfirm agreement on the overall plan and to coordinate its implementation, when warranted.

2124.04.3 COMMUNICATION AND COORDINATION AMONG SUPERVISORS TO DEVELOP AND ADMINISTER A SUPERVISORY PLAN

The communication process as described herein can serve as the basis for executing a comprehensive supervisory approach that capitalizes on the mandates and resources of the various supervisory authorities (for example, banking, securities, and insurance authorities), while minimizing possible duplication and burden on the BO. The objective is for supervisors to work cooperatively in developing supervisory plans and scope documents and, when possible and appropriate, to carry out important supervisory activities on a joint or coordinated basis. Coordination and communication among supervisors can reduce the burden on BOs and result in a more efficient deployment of supervisory resources.

An important element of the LCBO program is effective communication between the Federal Reserve and the BO's management throughout the supervision cycle. Communication with the LCBO can take various forms, including formal and informal meetings with management and the board of directors, as well as the issuance of periodic and annual supervisory reports, including examination or inspection reports, to the organization's management and board. The objective of these reports is to identify significant risks and summarize the Federal Reserve's view of the financial condition and effectiveness of the LCBO's risk-management processes.

As part of the LCBO program, the management of the BO should be encouraged to continue and, if warranted, strengthen communications with Reserve Bank management, CPCs, and the supervisory teams, particularly with respect to providing information to supervisors on a timely basis regarding material financial or operational issues or problems. BOs should also be encouraged to continuously review and enhance their public disclosures in order to promote transparency and foster effective market discipline. Also, if BOs promptly notify supervisors of emerging problems, they often can be resolved in a way that minimizes disruptions. Strong two-way communications and information flows between supervisors and the LCBO's senior management, including key business-line

and risk managers, are essential to the success of the LCBO program. In carrying out this program, the Federal Reserve will continue to assign its highest priority to information security and to protecting the integrity of sensitive, confidential supervisory information and examination or inspection information.

The LCBO supervisory framework also requires that results and findings of supervisory activities conducted throughout the supervisory cycle be continually evaluated and reflected in the Federal Reserve's current understanding and assessment of the organization's risk profile. Reports of examination or inspection or letters to the LCBO's management and board of directors should routinely be prepared when examinations, inspections, and targeted reviews are completed. If necessary, the organization's supervisory ratings should be revised in a timely manner, based on those findings.[2] Risk-management and composite supervisory ratings should be adjusted appropriately if material weaknesses in risk-management systems or controls exist, even if these weaknesses have not yet affected the organization's reported financial results.

At least annually, a comprehensive summary supervisory report should be prepared that supports the organization's assigned ratings and encompasses the results of the entire supervisory cycle. This report should convey the Federal Reserve's view of the condition of the LCBO and its key risk-management processes, communicate the composite supervisory rating(s), discuss each of the major business risks, summarize the supervisory activities conducted during the supervisory cycle and the resulting findings, and assess the effectiveness of any corrective actions taken by the LCBO. This report will satisfy supervisory and legal requirements for a full-scope examination or inspection. Reserve Bank management, as well as Board officials, when warranted, will meet with the LCBO's board of directors to present and discuss the contents of the report and the Federal Reserve's assessment of the condition of the BO.

2124.04.3.1 Information Sharing and Coordination with Supervisory Authorities and External and Internal Auditors

Information sharing and coordination within the Federal Reserve and with supervisors of major affiliates are critical elements of the LCBO program and are essential to successful supervision of LCBOs. Most LCBOs, regardless of their business lines and functional management structure, operate through a variety of legal entities that may be under the jurisdiction of different licensing and supervisory authorities in the United States and abroad.

To maximize efficiency and reduce regulatory burden, the risk-assessment and supervisory-planning processes should use and leverage off, or benefit from, the efforts of other principal supervisors to the extent possible, consistent with achieving the Federal Reserve's key supervisory objectives. The Reserve Bank responsible for the supervision of the LCBO should have regular contacts with supervisors of important affiliates of the organization to discuss and coordinate matters of common interest; to develop supervisory plans; and, when and where appropriate, to coordinate the scheduling and conduct of examinations, inspections, and targeted reviews. Consistent with the supervisory needs and responsibilities of the Federal Reserve and the other supervisors, information may be exchanged as permitted by law and in accordance with applicable rules and policies of the Board. In addition, meetings should be held at reasonable intervals with internal and external auditors to review audit plans, evaluate significant audit findings and other control assessments, and foster opportunities to leverage off the auditors' work. Building on the work of auditors, when and where appropriate, can enhance supervisory efficiency and reduce the regulatory burden on the LCBO.

2124.04.3.2 Enhanced Use of Information Technology

The Federal Reserve's supervisory approach for LCBOs continues to use enhanced information technology. Timely and user-friendly access to a full range of internal and third-party information, as well as mechanisms to foster collaboration among Federal Reserve staff and other supervisors, is essential to effective risk-focused supervision for LCBOs. Effective and timely information flows, facilitated by the use of enhanced information technology, can provide a way for supervisors to ''harvest'' and share the core knowledge and experience gained through the conduct of supervisory activities and through ongoing contacts with BOs. Ready

2. The supervisory ratings include the RFI/C(D) and CAMELS ratings, and an FBO's combined U.S. operations rating.

access to the collective knowledge, insights, and current assessments of fellow supervisors, bank management, financial markets, and other relevant third parties can enhance the ability of supervisors to identify problems in a timely manner and formulate effective supervisory responses. To this end, the Federal Reserve System's information-sharing and information technology strategies will continue to be aimed at broadening and strengthening the role of the CPCs, supervisory teams, and other System staff who are responsible for conducting and overseeing its supervisory programs, including the LCBO program.

2124.04.4 ORGANIZATION OF FEDERAL RESERVE SUPERVISORY TEAMS

A principal component of the supervisory framework is the assignment of a dedicated supervisory team to each LCBO. The teams are made up of individuals with specialized skills, which are based on the organization's particular business lines and risk profile. This full-time, dedicated cadre will be supplemented, as necessary, by other specialized System staff, who will participate in examinations and targeted reviews.

In addition to designing and executing the supervisory strategy for an LCBO, the CPC has responsibility for managing the supervisory team. Important objectives in managing the supervision resources for a particular LCBO are to maximize institutional knowledge and minimize burden to the BO, while maintaining an objective, ongoing understanding of the BO's risk profile. The CPC serves as the Federal Reserve's primary day-to-day contact for a particular LCBO and has, together with other members of the Reserve Bank management team, primary responsibility for communicating with senior officials of the LCBO.

The supervisory team's major responsibilities are to maintain a high level of knowledge on the BO and to ensure that supervisory strategies and priorities are consistent with the identified risks and the LCBO's profile. The team should include supervisors with broad-based knowledge and experience in banking, as well as specialists whose technical skills and market knowledge bring depth and perspective to highly focused reviews of selected LCBO activities.

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 board of directors' 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" (section 4070.1). This letter or section provides general guidance on risk-management processes and internal controls for consolidated organizations and discusses the elements of a sound risk-management system applicable to all banking organizations for which the Federal Reserve has supervisory responsibility. SR-95-51

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 addition to the oversight provided by the board of directors and various executive and management committees of an organization, a key component of firmwide compliance oversight in larger, more complex banking organizations 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.

states that all bank holding companies should be able to assess the major risks of the consolidated organization. See also 12 C.F.R. 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 board of directors may assign primary responsibility for aspects of the compliance program to other units within the organization (e.g., finance, information technology, human resources, etc.). 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. The board, senior management, and the corporate compliance function are responsible for working together to establish and implement a comprehensive and effective compliance risk-management program and oversight framework that is reasonably designed to prevent and detect compliance breaches and issues.

2124.07.4.1 Boards of Directors.[9]

Boards of directors are responsible for setting an appropriate culture of compliance within their organizations, for establishing clear policies regarding the management of key risks, and for ensuring that these policies are adhered to in practice. The following discussion is intended to clarify existing Federal Reserve supervisory 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.

To achieve its objectives, a sound and effective firmwide compliance risk-management program should have the support of the board and senior management. As set forth in applicable

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. 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.

law and supervisory guidance, the board and senior management of a banking organization have different, but complementary, roles in managing and overseeing compliance risk.[10]

The board has the responsibility for promoting a culture that encourages ethical conduct and compliance with applicable rules and standards. 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. The board should have an appropriate understanding of the types of compliance risks to which the organization is exposed. The level of technical knowledge required of directors to fulfill these responsibilities may vary, depending on the particular circumstances at the organization.

The board should ensure that senior management is fully capable, qualified, and properly motivated to manage the compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations. The board should ensure that its views about the importance of compliance are understood and communicated by senior management across, and at all levels of, the organization through ongoing training and other means. The board should ensure that senior management has established appropriate incentives to integrate compliance objectives into the management goals and compensation structure across the organization and that appropriate disciplinary actions and other measures are taken when serious compliance failures are identified. Finally, the board should ensure that the corporate compliance function has an appropriately prominent status within the organization. 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.

The board should be knowledgeable about the general content of the compliance program and exercise appropriate oversight of the program. Accordingly, the board should review and approve key elements of the organization's compliance risk-management program and oversight framework, including firmwide compliance policies, compliance risk-management standards, and roles and responsibilities of committees and functions with compliance oversight responsibilities. The board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by senior management. The board should exercise reasonable due diligence to ensure that the compliance program remains effective by at least annually reviewing a report on the effectiveness of the program. The board may delegate these tasks to an appropriate board-level committee.

2124.07.4.2 Senior Management

Senior management across the organization is responsible for communicating and reinforcing the compliance culture established by the board and for implementing measures to promote the culture. Senior management also should implement and enforce the compliance policies and compliance risk-management standards that have been approved by the board. 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 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.

10. See, for example, the Basel compliance paper; SR-04-18, "Bank Holding Company Rating System"(section 4070.0); SR-95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies"(section 4070.1); and the United States Sentencing Commission's *Federal Sentencing Guidelines Manual*, Chapter Eight, "Sentencing of Organizations."

The Federal Reserve had adopted risk-focused supervision frameworks for community banks and large complex banking organizations, including foreign banking organizations. 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 increasing dependency of banking organizations on the use of information technology, the Federal Reserve expects an organization's management and board of directors 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-98-09.

This section supplements further the guidance on the evaluation of banking organizations' risk-management processes. The primary objectives are to—

1. highlight the critical dependence of the financial services industry on information technology and its potential effect on safety and soundness,
2. reinforce the concept that the risk-focused supervisory process and related products (risk assessments, supervisory plans, and scope memoranda) for an organization must address the risks associated with its use of information technology,[3] and
3. provide 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

As the automated processing of information has moved beyond centralized mainframe operations to encompass end-user computer and distributed processing systems, the use of information technology in general has expanded greatly. In the banking industry, information technology was once limited to automation of routine transactions and preparation of financial reports but is now used to automate all levels of a banking organization's operations and information processing. Some decision-making processes such as credit scoring and securities trading have been fully automated. New, complex financial products are possible largely because of valuation models that depend on technology. 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 information technology, have placed increased emphasis on the management of this important resource. In large banking organizations, the positions of the chief information officer and chief technology officer have become more visible in the top executive ranks of banking organizations. In addition, managers of activities that rely on end-user computing and distributed processing systems

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. The supervisory products are described in SR-97-24 for large complex institutions and SR-97-25 for community banks.

have been assigned more direct responsibility for the information technology used in conducting their business. As a result, the management of the risks associated with information technology must 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 mainframe computer systems are still an integral part of the information technology on which many large banking organizations rely. This includes systems critical to the global payments system 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 review of the effectiveness and reliability of the critical mainframe systems and third-party processors will continue to be an important part of the Federal Reserve's supervisory activities.

2124.1.2 IMPLICATIONS FOR RISK-FOCUSED SUPERVISION

The risk-focused supervisory process is evolving and adapting to the changing role of information technology, with a greater emphasis being placed on an evaluation of information technology and an assessment of its effect on an organization's safety and soundness. Accordingly, examiners should explicitly consider information technology when developing their risk assessments and supervisory plans. It is expected that examiners will 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 close coordination is needed between general safety-and-soundness examiners and information technology specialists during the risk assessment and planning, as well as during the on-site phase of the examination or inspection. In general, examiners should take the following actions:

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.[4] 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 the board of directors and senior management are 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.[5]

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

4. These components include mainframe, local area network, and personal computers, as well as software applications.

5. 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.

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 the elements could have a substantive adverse effect on the organization's or activity's business risks. 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 business risks.

The elements are to be used as a flexible tool to facilitate consideration and discussion of the risks associated with information technology. Where an organization uses different terminology to describe information technology elements, examiners may use that terminology provided the organization adequately addresses all elements. 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 described below:

1. *Management processes.* Management processes[6] 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[7] 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

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

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 technology 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

While mainframe computer systems are still 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 network and personal computers. In contrast, many community and regional banks continue to rely on third-party information technology service centers. Given this variability of information technology environments, the level of technical expertise needed for a particular examination or inspection will vary and should be identified during its planning phase. For example, a specialist in information technology or the particular business activity may be the most appropriate person to review 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 continuous 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.

2124.1.5 INSPECTION OBJECTIVES

1. To assess the risks associated with information technology when developing the scope of supervisory plans and activities.
2. To consider the various risks associated with information technology along with the risk evaluation of the banking organization's business activities.
3. To assess the effectiveness of the risk-management process that the banking organization applies to information technology.
4. To view the banking organization's information technology elements in an integrated manner along with the overall business risks of the banking organization or its business activity, and ascertain if there are any deficiencies therein.

2124.1.6 INSPECTION PROCEDURES

1. Develop a broad understanding of the organization's approach, strategy, and structure with regard to information technology.
2. Incorporate an analysis of information technology systems into risk assessments, supervisory plans, and scope memoranda.
3. Assess the banking organization's critical systems and the degree of reliance those activities have on information technology systems.
4. Determine that the information systems are delivering the services necessary for the organization to conduct its business safely and soundly.
5. Determine if the board of directors or senior management has conducted an independent review, either by independent qualified staff or by an independent third-party consultant, of the current architecture, assessing the risks

associated with the institution's information technology. Did the review establish whether the organization's architecture had provided for—

a. current and long-term organizational objectives,
b. capacity requirements during normal and peak processing periods,
c. solutions when information is stored and processed in two or more separate systems,
d. the hardware's capability to run the software and its compatibility and integration with other systems and sources of data,
e. the ability to upgrade to higher levels of performance and capacity, and
f. the adequacy of controls.

6. Determine if the institution relies on information system audits or independent application reviews to determine whether information flows are accurate and complete.
7. Review, on a sample basis, the reliability, accuracy, and completeness of processed delivered information.
8. Determine whether the 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.
9. Determine whether the board of directors and senior management are adequately identifying, measuring, monitoring, and controlling the significant risks associated with information technology for the overall banking organization and its major business activities.
10. After developing an understanding of the banking organization, assess and comment on the information technology risks and management in a scope memorandum.

2124.1.7 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.

WHAT'S NEW IN THIS REVISED SECTION

Effective July 2006, footnote 12 was revised to include a reference to SR-00-14, "Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign Banking Organizations."

Effective January 2006, this section, previously titled "Standards for Safeguarding Customer Information," has been retitled "Information Security Standards" to conform with an interagency final rule that implements section 216 of the Fair and Accurate Credit Transactions Act of 2003. The Interagency Guidelines Establishing Information Security Standards, as amended December 16, 2004, generally require each bank holding company 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 in order to address the risks associated with identity theft. (See 12 C.F.R. 225, appendix F.) The amendments to the information security standards were effective July 1, 2005.

The section has also been revised to incorporate the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the guidance), which was jointly issued on March 23, 2005 (effective March 29, 2005), by the adopting agencies. The guidance describes the response programs, including customer notification procedures, that a bank holding company 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. (See SR-05-23/CA-05-10.)

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

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.

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 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

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

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-

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.[15] 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,[16] 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,[17] 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 Suspicious Activity Report (SAR) was or will be

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. See SR-97-32, ''Sound Practices Guidance for Information Security for Networks,'' for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

16. See SR-00-04, ''Outsourcing of Information and Transaction Processing.''

17. 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-03-12, ''Revisions to the Suspicious Activity Report Form,'' and SR-01-11, ''Identity Theft and Pretext Calling.''

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 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.[18] 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.)[19]

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.

18. 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.

19. The FTC web site for the ID theft brochure and the FTC hotline phone number are www.consumer.gov/idtheft/ 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).

The review of risk management and internal controls is an essential element of the inspection or examination of trading activities. In view of the increasing importance of these activities to the overall risk profile and profitability of certain banking organizations,[2] this guidance highlights key considerations when inspecting or examining the risk management and internal controls of trading activities in both cash and derivative instruments.[3]

The principles set forth in this guidance apply to the risk management practices of bank holding companies, which should manage and control aggregate risk exposures on a consolidated basis while recognizing legal distinctions among subsidiaries. This guidance is specifically designed to target trading, market making, and customer accommodation activities in cash and derivative instruments at state member banks, branches and agencies of foreign banks, and Edge corporations. Many of the principles advanced can also be applied to banking organizations' use of derivatives as end-users. Examiners should assess management's application of this guidance to the holding company and to a banking organization's end-user derivative activities where appropriate, given the nature of the organization's activities and current accounting standards.

This examiner guidance is specifically provided for evaluating the following elements of an organization's risk management process for trading and derivatives activities:

- Board of directors and management oversight
- The measurement procedures, limit systems, and monitoring and review functions of the risk management process
- Internal controls and audit procedures

In assessing the adequacy of these elements at individual institutions, examiners should consider the nature and volume of a banking organization's activities and its overall approach toward managing the various types of risks involved. As with the inspection of other activities, examiner judgment plays a key role in assessing the adequacy and necessary sophistication of a banking organization's risk management system for cash and derivative instrument trading and hedging activities.

Many of the managerial practices and examiner procedures contained in this guidance are fundamental and are generally accepted as sound banking practices for both trading and nontrading activities. However, other elements may be subject to change, as both supervisory and bank operating standards evolve in response to new technologies, financial innovations, and developments in market and business practices.

2125.0.1 OVERSIGHT OF THE RISK MANAGEMENT PROCESS

As is standard practice for most banking activities, banking organizations should maintain written policies and procedures that clearly outline the organization's risk management guidance for trading and derivative activities. At a minimum these policies should identify the risk tolerances of the board of directors and should clearly delineate lines of authority and responsibility for managing the risk of these activities. Individuals throughout the trading and derivatives areas should be fully aware of all policies and procedures that relate to their specific duties.

The board of directors, senior-level management, and members of independent risk management functions are all important participants in the risk management process. Examiners should ensure that these participants are aware of their responsibilities and that they adequately perform their appropriate role in managing the risk of trading and derivative activities.

2125.0.1.1 Board of Directors' Approval of Risk Management Policies

The board of directors should approve all significant policies relating to the management of risks throughout the organization. These policies, which should include those related to trading activities, should be consistent with the organization's broader business strategies, capital adequacy, expertise, and overall willingness

1. The following is the text of SR-93-69, adapted for this manual. Section numbers have been added for reference.

2. The term "banking organizations" refers to institutions or entities that are directly supervised by the Board of Governors of the Federal Reserve System, such as state member banks and bank holding companies, including the nonbank subsidiaries of the holding company.

3. In general terms, derivative instruments are bilateral contracts or agreements whose value derives from the value of one or more underlying assets, interest rates, exchange rates, commodities, or financial or commodity indexes.

to take risk. Accordingly, the board should be informed regularly of risk exposure and should regularly reevaluate significant risk management policies and procedures with special emphasis placed on those defining the institution's risk tolerance regarding these activities. The board of directors should also conduct and encourage discussions between its members and senior management, as well as between senior management and others in the organization, regarding its risk management process and risk exposure.

2125.0.1.2 Senior Management's Risk Management Responsibilities

Senior management is responsible for ensuring that there are adequate policies and procedures for conducting trading operations on both a long-range and day-to-day basis. This responsibility includes ensuring that there are clear delineations of lines of responsibility for managing risk, adequate systems for measuring risk, appropriately structured limits on risk taking, effective internal controls, and a comprehensive risk-reporting process.

Senior management should regularly evaluate the procedures in place to manage risk to ensure that those procedures are appropriate and sound. Senior management should also foster and participate in active discussions with the board, with staff of risk management functions, and with traders regarding procedures for measuring and managing risk. Management must also ensure that trading and derivative activities are allocated sufficient resources and staff to manage and control risks.

2125.0.1.3 Independent Risk Management Functions

The process of measuring, monitoring, and controlling risk consistent with the established policies and procedures should be managed independently of individuals conducting trading activities, up through senior levels of the institution. An independent system for reporting exposures to both senior-level management and to the board of directors is an important element of this process.

Banking organizations should have highly qualified personnel throughout their trading and derivatives areas, including their risk management and internal control functions. The personnel staffing independent risk management functions should have a complete understanding of the risks associated with all traded on- and off-balance-sheet instruments. Accordingly, compensation policies for these individuals should be adequate to attract and retain personnel qualified to judge these risks. As a matter of general policy, compensation policies, especially in the risk management, control, and senior management functions, should be structured in a way that avoids the potential incentives for excessive risk taking that can occur if, for example, salaries are tied too closely to the profitability of trading or derivatives activities.

2125.0.2 THE RISK MANAGEMENT PROCESS

The primary components of a sound risk management process are a comprehensive risk measurement approach; a detailed structure of limits, guidelines, and other parameters used to govern risk taking; and a strong management information system for monitoring and reporting risks. These components are fundamental to both trading and nontrading activities alike. Moreover, the underlying risks associated with these activities, such as credit, market, liquidity, and operating risk, are not new to banking organizations, although their measurement and management can be somewhat more complex. Accordingly, the process of risk management for trading activities should be integrated into the organization's overall risk management system to the fullest extent possible using a conceptual framework common to its other activities. Such a common framework enables the organization to manage its consolidated risk exposure more effectively, especially since the various individual risks involved in trading activities can, at times, be interconnected and can often transcend specific markets.

As is the case with all risk-bearing activities, the risk exposures a banking organization assumes in its trading and derivatives activities should be fully supported by an adequate capital position. Banking organizations should ensure that their capital positions are sufficiently strong to support all trading and derivatives risks on a fully consolidated basis and that adequate capital is maintained in all affiliated entities engaged in these activities.

2125.0.2.1 Risk Measurement Systems

A banking organization's system for measuring

the various risks of trading and derivatives activities should be both comprehensive and accurate. Risks should be measured and aggregated across trading and nontrading activities on an organizationwide basis to the fullest extent possible.

While examiners should not require the use of a single prescribed risk measurement approach for management purposes, they should evaluate the extent to which the organization's procedures enable management to assess exposures on a consolidated basis. Examiners should also evaluate whether the risk measures and the risk measurement process are sufficiently robust to accurately reflect the multiple types of risks facing the banking organization. Risk measurement standards should be understood by relevant personnel at all levels—from individual traders to the board of directors—and should provide a common framework for limiting and monitoring risk-taking activities.

The process of marking trading and derivatives positions to market is fundamental to measuring and reporting exposures accurately and on a timely basis. Banking organizations active in dealing in foreign exchange, derivatives, and other traded instruments should have the ability to monitor credit exposures, trading positions, and market movements at least daily. Some organizations should also have the capacity, or at least the goal, of monitoring their more actively traded products on a real-time basis.

Analyzing stress situations, including combinations of market events that could affect the banking organization, is also an important aspect of risk measurement. Sound risk measurement practices include identifying possible events or changes in market behavior that could have unfavorable effects on the organization and assessing its ability to withstand them. These analyses should consider not only the likelihood of adverse events, reflecting their probability, but also plausible ''worst-case'' scenarios. Ideally, such worst-case analysis should be conducted on an organizationwide basis by taking into account the effect of unusual price changes or the default of a large counterparty across both the derivatives and cash-trading portfolios and the loan and funding portfolios.

Such stress tests should not be limited to quantitative exercises that compute potential losses or gains. They should also include more qualitative analyses of the actions management might take under particular scenarios. Contingency plans outlining operating procedures and lines of communication, both formal and informal, are important products of such qualitative analyses.

2125.0.2.2 Limiting Risks

A sound system of integrated organizationwide limits and risk-taking guidelines is an essential component of the risk management process. Such a system should set boundaries for organizational risk-taking and should also ensure that positions that exceed certain predetermined levels receive prompt management attention, so that they can be either reduced or prudently addressed. The limit system should be consistent with the effectiveness of the organization's overall risk management process and with the adequacy of its capital position. An appropriate limit system should permit management to control exposures, to initiate discussion about opportunities and risks, and to monitor actual risk-taking against predetermined tolerances, as determined by the board of directors and senior management.

Global limits should be set for each major type of risk involved. These limits should be consistent with the banking organization's overall risk measurement approach and should be integrated to the fullest extent possible with organizationwide limits on those risks as they arise in all other activities of the firm. The limit system should provide the capability to allocate limits down to individual business units.

At times, especially when markets are volatile, traders may exceed their limits. While such exceptions may occur, they should be made known to senior management and approved only by authorized personnel. These positions should also prompt discussions between traders and management about the consolidated risk-taking activities of the firm or the trading unit. The seriousness of individual or continued limit exceptions depends in large part upon management's approach toward setting limits and on the actual size of individual and organizational limits relative to the organization's capacity to take risk. Banking organizations with relatively conservative limits may encounter more exceptions to those limits than do organizations where limits may be less restrictive. Ultimately, examiners should ensure that stated policies are enforced and that the level of exposure is managed prudently.

2125.0.2.3 Reporting

An accurate, informative, and timely management information system is essential to the pru-

dent operation of a trading or derivatives activity. Accordingly, the examiner's assessment of the quality of the management information system is an important factor in the overall evaluation of the risk management process. Examiners should determine the extent to which the risk management function monitors and reports its measures of trading risks to appropriate levels of senior management and to the board of directors. Exposures and profit and loss statements should be reported at least daily to managers who supervise but do not, themselves, conduct trading activities. More frequent reports should be made as market conditions dictate. Reports to other levels of senior management and the board may occur less frequently, but examiners should determine whether the frequency of reporting provides these individuals with adequate information to judge the changing nature of the organization's risk profile.

Examiners should ensure that the management information systems translate the measured risk from a technical and quantitative format to one that can be easily read and understood by senior managers and directors, who may not have specialized and technical knowledge of trading activities and derivative products. Risk exposures arising from various products within the trading function should be reported to senior managers and directors using a common conceptual framework for measuring and limiting risks.

2125.0.2.4 Management Evaluation and Review of the Risk Management Process

Management should ensure that the various components of an organization's risk management process are regularly reviewed and evaluated. This review should take into account changes in the activities of the organization and in the market environment, since the changes may have created exposures that require additional management and examiner attention. Any material changes to the risk management system should also be reviewed.

The independent risk management functions should regularly assess the methodologies, models, and assumptions used to measure risk and to limit exposures. Proper documentation of these elements of the risk measurement system is essential for conducting meaningful reviews. The review of limit structures should compare limits to actual exposures and should also consider whether existing measures of exposure and limits are appropriate in view of the banking organization's past performance and current capital position.

The frequency and extent to which banking organizations should reevaluate their risk measurement methodologies and models depends, in part, on the specific risk exposures created by their trading activities, on the pace and nature of market changes, and on the pace of innovation with respect to measuring and managing risks. At a minimum, banking organizations with significant trading and derivative activities should review the underlying methodologies of their models at least annually—and more often as market conditions dictate—to ensure they are appropriate and consistent. Such internal evaluations may, in many cases, be supplemented by reviews by external auditors or other qualified outside parties, such as consultants who have expertise with highly technical models and risk management techniques. Assumptions should be evaluated on a continual basis.

Banking organizations should also have an effective process to evaluate and review the risks involved in products that are either new to the firm or new to the marketplace and of potential interest to the firm. In general, a banking organization should not trade a product until senior management and all relevant personnel (including those in risk management, internal control, legal, accounting, and auditing) understand the product and are able to integrate the product into the banking organization's risk measurement and control systems. Examiners should determine whether the banking organization has a formal process for reviewing new products and whether it introduces new products in a manner that adequately limits potential losses.

2125.0.2.5 Managing Specific Risks

The following discussions present examiner guidance for evaluating the specific components of a firm's risk management process in the context of each of the risks involved in trading cash and derivatives instruments.

2125.0.2.5.1 Credit Risk

Broadly defined, credit risk is the risk that a counterparty will fail to perform on an obligation to the banking organization. Banking organizations should evaluate both settlement and

presettlement credit risk at the customer level across all traded derivative and nonderivative products. On settlement day, the exposure to counterparty default may equal the full value of any cash flows or securities the banking organization is to receive. Prior to settlement, credit risk is measured as the sum of the replacement cost of the position, plus an estimate of the banking organization's potential future exposure from the instrument as a result of market changes. Replacement cost should be determined using current market prices or generally accepted approaches for estimating the present value of future payments required under each contract, given current market conditions.

Potential credit-risk exposure is measured more subjectively than current exposure and is primarily a function of the time remaining to maturity and the expected volatility of the price, rate, or index underlying the contract. It is often assessed through simulation analysis and option-valuation models, but can also be addressed by using ''add-ons,'' such as those included in the risk-based capital standard. In either case, examiners should evaluate the reasonableness of the assumptions underlying the banking organization's risk measure and should also ensure that banking organizations that measure exposures using a portfolio approach do so in a prudent manner.

Master netting agreements and various credit enhancements, such as collateral or third-party guarantees, can be used by banking organizations to reduce their counterparty credit risk. In such cases, a banking organization's credit exposures should reflect these risk-reducing features only to the extent that the agreements and recourse provisions are legally enforceable in all relevant jurisdictions. This legal enforceability should extend to any insolvency proceedings of the counterparty. Banking organizations should be able to demonstrate that they have exercised due diligence in evaluating the enforceability of these contracts and that individual transactions have been executed in a manner that provides adequate protection.

Credit limits that consider both settlement and presettlement exposures should be established for all counterparties with whom the banking organization trades. As a matter of general policy, trading with a counterparty should not commence until a credit line has been approved. The structure of the credit-approval process may differ among organizations, reflecting the organizational and geographic structure of the organization and the specific needs of its trading activities. Nevertheless, in all cases, it is important that credit limits be determined by personnel who are independent of the trading function, that these personnel use standards that are consistent with those used for nontrading activities, and that counterparty credit lines are consistent with the organization's policies and consolidated exposures.

Examiners should consider the extent to which credit limits are exceeded and whether exceptions were resolved according to the banking organization's adopted policies and procedures. Examiners should also evaluate whether the organization's reports adequately provide traders and credit officers with relevant, accurate, and timely information about the credit exposures and approved credit lines.

Trading activities that involve cash instruments often involve short-term exposures that are eliminated at settlement. However, in the case of derivative products traded in over-the-counter markets, the exposure can often exist for a period similar to that commonly associated with a loan from a banking organization. Given this potentially longer-term exposure and the complexity associated with some derivative instruments, banking organizations should consider not only the overall financial strength of the counterparty and its ability to perform on its obligation, but should also consider the counterparty's ability to understand and manage the risks inherent in the derivative product.

2125.0.2.5.2 Market Risk

Market risk is the risk to a banking organization's financial condition resulting from adverse movements in market prices. Accurately measuring a banking organization's market risk requires timely information about the current market values of its assets, liabilities, and off-balance-sheet positions. Although there are many types of market risks that can affect a portfolio's value, they can generally be described as those involving forward risk and those involving options. Forward risks arise from factors such as changing interest rates and currency exchange rates, the liquidity of markets for specific commodities or financial instruments, and local or world political and economic events. Market risks related to options include these factors as well as evolving perceptions of the volatility of price changes, the passage of time, and the interactive effect of other market risks. All of these sources of potential market risk can affect the value of the organiza-

tion and should be considered in the risk measurement process.

Market risk is increasingly measured by market participants using a value-at-risk approach, which measures the potential gain or loss in a position, portfolio, or organization that is associated with a price movement of a given probability over a specified time horizon. Banking organizations should revalue all trading portfolios and calculate their exposures at least daily. Although banking organizations may use risk measures other than value at risk, examiners should consider whether the measure used is sufficiently accurate and rigorous and whether it is adequately incorporated into the banking organization's risk management process.

Examiners should also ensure that the organization compares its estimated market-risk exposures with actual market-price behavior. In particular, the output of any market-risk models that require simulations or forecasts of future prices should be compared with actual prices. If the projected and actual results differ materially, the models should be modified, as appropriate.

Banking organizations should establish limits for market risk that relate to their risk measures and that are consistent with maximum exposures authorized by their senior management and board of directors. These limits should be allocated to business units and individual traders and be clearly understood by all relevant parties. Examiners should ensure that exceptions to limits are detected and adequately addressed by management. In practice, some limit systems may include additional elements such as stop-loss limits and trading guidelines that may play an important role in controlling risk at the trader and business-unit level; examiners should include them in their review of the limit system.

2125.0.2.5.3 Liquidity Risk

Banking organizations face two types of liquidity risk in their trading activities: those related to specific products or markets and those related to the general funding of the banking organization's trading activities. The former is the risk that a banking organization cannot easily unwind or offset a particular position at or near the previous market price because of inadequate market depth or because of disruptions in the marketplace. Funding-liquidity risk is the risk that the banking organization will be unable to meet its payment obligations on settlement dates. Since neither type of liquidity risk is unique to trading activities, management should evaluate these risks in the broader context of the organization's overall liquidity. When establishing limits, organizations should be aware of the size, depth, and liquidity of the particular market and establish trading guidelines accordingly. Management should also give consideration to the potential problems associated with replacing contracts that terminate early in volatile or illiquid markets.

In developing guidelines for controlling the liquidity risks in trading activities, banking organizations should consider the possibility that they could lose access to one or more markets, either because of concerns about the banking organization's own creditworthiness, the creditworthiness of a major counterparty, or because of generally stressful market conditions. At such times, the banking organization may have less flexibility in managing its market-, credit-, and liquidity-risk exposures. Banking organizations that make markets in over-the-counter derivatives or that dynamically hedge their positions require constant access to financial markets, and that need may increase in times of market stress. The banking organization's liquidity plan should reflect the organization's ability to turn to alternative markets, such as futures or cash markets, or to provide sufficient collateral or other credit enhancements in order to continue trading under a broad range of scenarios.

Examiners should ensure that banking organizations that participate in over-the-counter derivative markets adequately consider the potential liquidity risks associated with the early termination of derivative contracts. Many forms of standardized contracts for derivative transactions allow counterparties to request collateral or to terminate their contracts early if the banking organization experiences an adverse credit event or a deterioration in its financial condition. In addition, under conditions of market stress, customers may ask for the early termination of some contracts within the context of the dealer's market-making activities. In such situations, a banking organization that owes money on derivative transactions may be required to deliver collateral or settle a contract early and possibly at a time when the banking organization may face other funding and liquidity pressures. Early terminations may also open up additional, unintended, market positions. Management and directors should be aware of these potential liquidity risks and should address them in the banking organization's liquidity plan and in the broader context of the

banking organization's liquidity management process. In their reviews, examiners should consider the extent to which such potential obligations could present liquidity risks to the banking organization.

2125.0.2.5.4 Operational Risk, Legal Risk, and Business Practices

Operating risk is the risk that deficiencies in information systems or internal controls will result in unexpected loss. Legal risk is the risk that contracts are not legally enforceable or documented correctly. Although operating and legal risks are difficult to quantify, they can often be evaluated by examining a series of plausible ''worst-case'' or ''what-if'' scenarios, such as a power loss, a doubling of transaction volume, a mistake found in the pricing software for collateral management, or an unenforceable contract. They can also be assessed through periodic reviews of procedures, documentation requirements, data processing systems, contingency plans, and other operating practices. Such reviews may help to reduce the likelihood of errors and breakdowns in controls, improve the control of risk and the effectiveness of the limit system, and prevent unsound marketing practices and the premature adoption of new products or lines of business. Considering the heavy reliance of trading activities on computerized systems, banking organizations should have plans that take into account potential problems with their normal processing procedures.

Banking organizations should also ensure that trades that are consummated orally are confirmed as soon as possible. Oral transactions conducted via telephone should be recorded on tape and subsequently supported by written documents. Examiners should ensure that the organization monitors the consistency between the terms of a transaction as they were orally agreed upon and the terms as they were subsequently confirmed.

Examiners should also consider the extent to which banking organizations evaluate and control operating risks through the use of internal audits, stress testing, contingency planning, and other managerial and analytical techniques. Banking organizations should also have approved policies that specify documentation requirements for trading activities and formal procedures for saving and safeguarding important documents that are consistent with legal requirements and internal policies. Relevant personnel should fully understand the requirements.

Legal risks should be limited and managed through policies developed by the organization's legal counsel (typically in consultation with officers in the risk management process) that have been approved by the banking organization's senior management and board of directors. At a minimum, there should be guidelines and processes in place to ensure the enforceability of counterparty agreements. Examiners should determine whether a banking organization is adequately evaluating the enforceability of its agreements before individual transactions are consummated. Banking organizations should also ensure that the counterparty has sufficient authority to enter into the transaction and that the terms of the agreement are legally sound. Banking organizations should further ascertain that their netting agreements are adequately documented, that they have been executed properly, and that they are enforceable in all relevant jurisdictions. Banking organizations should have knowledge of relevant tax laws and interpretations governing the use of these instruments. Knowledge of these laws is necessary not only for the banking organization's marketing activities, but also for its own use of derivative products.

Sound business practices provide that banking organizations take steps to ascertain the character and financial sophistication of counterparties. This includes efforts to ensure that the counterparties understand the nature of and the risks inherent in the agreed transactions. Where the counterparties are unsophisticated, either generally or with respect to a particular type of transaction, banking organizations should take additional steps to ensure that counterparties are made aware of the risks attendant in the specific type of transaction. While counterparties are ultimately responsible for the transactions into which they choose to enter, where a banking organization recommends specific transactions for an unsophisticated counterparty, the banking organization should ensure that it has adequate information regarding its counterparty on which to base its recommendation.

2125.0.3 INTERNAL CONTROLS AND AUDITS

A review of internal controls has long been central to the Federal Reserve's examination and inspection of trading and derivatives activities. Policies and related procedures for the operation of these activities should be an exten-

sion of the organization's overall structure of internal controls and should be fully integrated into routine work-flows. Properly structured, a system of internal controls should promote effective and efficient operations, reliable financial and regulatory reporting, and compliance with relevant laws, regulations, and banking organization policies. In determining whether internal controls meet those objectives, examiners should consider the overall control environment of the organization; the process for identifying, analyzing, and managing risk; the adequacy of management information systems; and adherence to control activities such as approvals, confirmations, and reconciliations.

Assessing the adequacy of internal controls involves a process of understanding, documenting, evaluating, and testing an organization's internal control system. This assessment should include product- or business-line reviews which, in turn, should start with an assessment of the line's organizational structure. Examiners should check for adequate separation of duties, especially between trading desk personnel and internal control and risk management functions, adequate oversight by a knowledgeable manager without day-to-day trading responsibilities, and the presence of separate reporting lines for risk management and internal control personnel on one side and for trading personnel on the other. Product-by-product reviews of management structure should supplement the overall assessment of the organizational structure of the trading and derivatives areas.

Examiners are expected to conduct in-depth reviews of the internal controls of key activities. For example, for transaction recording and processing, examiners should evaluate written policies and procedures for recording trades, assess the trading area's adherence to policy, and analyze the transaction processing cycle, including settlement, to ensure the integrity and accuracy of the banking organization's records and management reports. Examiners should review the revaluation process in order to assess the adequacy of written policies and procedures for revaluing positions and for creating any associated revaluation reserves. Examiners should review compliance with revaluation policies and procedures, the frequency of revaluation, and the independence and quality of the sources of revaluation prices, especially for instruments traded in illiquid markets. All significant internal controls associated with the management of market risk, such as position versus limit reports and limit overage approval policies and procedures, should also be reviewed. Examiners should also review the credit approval process to ensure that the risks of specific products are adequately captured and that credit approval procedures are followed for all transactions.

An important step in the process of reviewing internal controls is the examiner's appraisal of the frequency, scope, and findings of independent internal and external auditors and the ability of those auditors to review the banking organization's trading and derivatives activities. Internal auditors should audit and test the risk management process and internal controls on a periodic basis, with the frequency based on a careful risk assessment. The depth and frequency of internal audits should be increased if weaknesses and significant issues are discovered or if significant changes have been made to product lines, modeling methodologies, the risk oversight process, internal controls, or the overall risk profile of the organization.

In reviewing the risk management functions in particular, internal auditors should thoroughly evaluate the effectiveness of internal controls relevant to measuring, reporting, and limiting risks. Internal auditors should also evaluate compliance with risk limits and the reliability and timeliness of information reported to the banking organization's senior management and board of directors. Internal auditors are also expected to evaluate the independence and overall effectiveness of the banking organization's risk management functions.

The level of confidence that examiners place in the banking organization's audit programs, the nature of the audit findings, and management's response to those findings will influence the scope of the current examination of trading and derivatives activities. Even when the audit process and findings are satisfactory, examiners should document, evaluate, and test critical internal controls.

Similar to the focus of internal auditors, examiners should pay special attention to significant changes in product lines, risk measurement methodologies, limits, and internal controls that have occurred since the last examination. Meaningful changes in earnings from trading or derivatives activities, or in the size of positions or the value at risk associated with these activities, should also receive emphasis during the inspection or examination.

WHAT'S NEW IN THIS REVISED SECTION

Effective January 2007, this section was revised to delete a reference to SR-95-17 that was superseded by SR-98-12, or the former section 2126.0. A reference to the previous 1992 Supervisory Policy Statement on Securities Activities is also deleted.

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, the Office of Thrift Supervision, 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.

2126.1.1.2 Scope

This guidance applies to all securities in *held-to-*

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.

maturity and *available-for-sale* accounts as defined in the Statement of Financial Accounting Standards No.115 (FAS 115), 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 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 applica-

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.

ble. 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 current 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

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).

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 legally required to meet certain quality standards (i.e., investment grade) for security purchases. Many institutions maintain and update ratings reports from one of the major 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.

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.

2126.3.3 ASSESSMENT OF COUNTERPARTY CREDITWORTHINESS

Supervisors and examiners should increase their

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.

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 counter-

party 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.

CollateraIization 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.

WHAT NEW IN THIS REVISED SECTION

Effective July 2006, footnote 1 was revised to include a reference to SR-00-14, "Enhancements to the Interagency Program for Supervising the U.S. Operations of Foreign Banking Organizations."

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 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 bank holding company'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 bank holding company'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 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 interest-rate risk, which will form the basis for ongoing evaluation of the adequacy of interest-rate risk 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 interest-rate risk.[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 interest-rate risk.

Although the guidance targets interest-rate risk management at commercial banks and Edge Act corporations, the basic principles presented in the policy statement are to be applied to bank holding companies. Bank holding companies 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 bank holding company's overall risk-management rating. Bank holding company examiners should refer to section 4090.1 of the *Commercial Bank Examination Manual* for more detailed inspection guidance on the joint policy statement on interest-rate risk.

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."