HT 10833(a)

FEDERAL RESERVE BANK OF NEW YORK

NEW YORK, N.Y. 10045-0001

AREA CODE 212-720-1830

January 29, 1996

TO THE CHIEF EXECUTIVE OFFICER OF BANK HOLDING COMPANIES
AND STATE MEMBER BANKS IN THE SECOND DISTRICT

SUBJECT: New Supervisory Procedures for Rating the Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies

Attached are recently developed guidelines that direct examiners, beginning in 1996, to provide separate supervisory ratings for the risk management process, including its system of internal controls, of all bank holding companies and state member banks. While examiners have long taken the quality of risk management and internal controls into account in evaluating an institution's overall condition, this new rating is intended to highlight in the examination process the importance of risk management and to facilitate appropriate supervisory follow-up actions. Examiners will give this rating significant weight when determining the rating of management under the CAMEL or BOPEC rating systems and also are directed to discuss their findings regarding an institution's risk management process with management, especially if they view the process as less than satisfactory. Examiners will also analyze the overall internal control structure of the organization in assessing the ability of management to effectively manage the institution. It is management's responsibility to establish an overall internal control framework appropriate for the size and complexity of an institution's operations.

The guidelines stress the importance of sound risk management and emphasize the need for adequate internal controls and segregation of duties. They draw from long-standing supervisory procedures that have been updated by policy statements and examination manuals in recent years to reflect new financial instruments and evolving market practices. They also stress that the Federal Reserve will take appropriate supervisory action if institutions fail to maintain adequate controls, including the separation of critical duties.

With the concurrence of Supervision Staff at the Board of Governors, we are supplementing the guidance to examiners in the final section, "Reporting Conclusions". This section provides direction to examiners for including comments, conclusions and criticisms, as well as an overall evaluation, of risk management and internal controls in discussions with management and within the

examination report. To reflect the importance we assign to internal controls, we have asked our examiners to make separate evaluations of risk management and internal controls before combining these assessments into an overall evaluation, and to include commentary on both risk management and internal controls in the examination report. With this approach, we hope to enhance the information provided bank management about the examiners' assessment of the bank's internal control environment, as well as its risk management systems.

If you have any questions about these procedures, please call me at (212) 720-1830 or Roseanne Farley, Supervising Examiner, Advisory and Technical Services Function, at (212) 720-2325.

Very truly yours,

Christine M. Cumming

Christine M. Cumming
Senior Vice President

Attachment

# Federal Reserve Guidelines for Rating Risk Management at State Member Banks and Bank Holding Companies

## OVERVIEW

Taking and managing risks are fundamental to the business of banking. Accordingly, the Federal Reserve has always placed significant supervisory emphasis on the adequacy of an institution's management of risk, including its system of internal controls, when evaluating the management at state member banks and bank holding companies. An institution's failure to establish a management structure that adequately identifies, measures, monitors, and controls the risks involved in its various products and lines of business has long been considered unsafe and unsound conduct. Principles of sound management should apply to the entire spectrum of risks facing a banking institution including, but not limited to, credit, market, liquidity, operational, legal, and reputational risk:

- ***Credit risk*** arises from the potential that a borrower or counterparty will fail to perform on an obligation.

- ***Market risk*** is the risk to a financial institution's condition resulting from adverse movements in market rates or prices, such as interest rates, foreign exchange rates, or equity prices.

- ***Liquidity risk*** 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 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").

- ***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.

- ***Legal risk*** arises from the potential that unenforceable contracts, lawsuits, or adverse judgements can disrupt or otherwise negatively affect the operations or condition of a banking organization.

- ***Reputational risk*** 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.

These risks and the banking activities associated with them are addressed in greater detail in the Commercial Bank Examination and Bank Holding Company Supervision Manuals, the Trading Activities Manual, and other guidance. In practice, an institution's business activities present various combinations and concentrations of these risks depending on the nature and scope of the particular activity. The following discussion provides guidelines for determining a rating for management's formal or informal systems for identifying, measuring and containing these risks.

## ELEMENTS OF RISK MANAGEMENT

When rating the quality of risk management at state member banks and bank holding companies as part of the evaluation of the overall quality of management, examiners should place primary consideration on findings relating to the following elements of a sound risk management system:

- active board and senior management oversight;
- adequate policies, procedures, and limits;
- adequate risk measurement, monitoring, and management information systems; and
- comprehensive internal controls

Each of these elements is described further below, along with a list of considerations relevant to assessing the adequacy of each element.

Examiners should recognize that the considerations specified in these guidelines are intended only to assist in the evaluation of risk management practices, and not as a checklist of requirements for each institution. Moreover, while all bank holding companies should be able to assess the major risks of the consolidated organization, examiners should expect parent companies that centrally manage the operations and functions of their subsidiary banks to have more comprehensive, detailed, and developed risk management systems than companies that delegate the management of risks to relatively autonomous banking subsidiaries.

Adequate risk management programs can vary considerably in sophistication, depending on the size and complexity of the banking organization and the level of risk that it accepts. For smaller institutions engaged solely in traditional banking activities and whose senior managers and directors are actively involved in the details of day-to-day operations, relatively basic risk management systems may be adequate. In such institutions, these systems may consist only of written policies addressing material areas of operations such as lending or investing, basic internal control

systems, and a limited set of management and board reports. However, large multinational organizations will require far more elaborate and formal risk management systems in order to address their broader and typically more complex range of financial activities and to provide senior managers and directors with the information they need to monitor and direct day-to-day activities. In addition to the banking organization's market and credit risks, risk management systems should also encompass the organization's trust and fiduciary activities, including investment advisory, mutual funds, and securities lending activities.

The risk management processes of large banking organizations would typically contain detailed guidelines that set specific prudential limits on the principal types of risks relevant to their activities worldwide. Furthermore, because of the diversity of their activities and the geographic dispersion of their operations, these institutions will require timely and relatively more sophisticated reporting systems in order to manage their risks properly. These reporting systems, in turn, should comprise an adequate array of reports that provide the levels of detail about risk exposures that are relevant to the duties and responsibilities of individual managers and directors.

Such extensive systems of large institutions will naturally require frequent monitoring and testing by independent control areas and internal, as well as external, auditors to ensure the integrity of the information used by senior officials in overseeing compliance with policies and limits. The risk management systems or units of such institutions must also be sufficiently independent of the business lines in order to ensure an adequate separation of duties and the avoidance of conflicts of interest.

**Active Board and Senior Management Oversight**

Boards of directors have ultimate responsibility for the level of risk taken by their institutions. Accordingly, they should approve the overall business strategies and significant policies of their organizations, including those related to managing and taking risks, and should also ensure that senior management is fully capable of managing the activities that their institutions conduct. While all boards of directors are responsible for understanding the nature of the risks significant to their organizations and for ensuring that management is taking the steps necessary to identify, measure, monitor, and control these risks, the level of technical knowledge required of directors may vary depending on the particular circumstances at the institution.

Directors of large banking organizations that conduct a broad range of technically complex activities, for example, cannot be expected to understand the full details of their institutions' activities or the precise ways risks are measured and controlled. They should, however, have a clear understanding of the types of risks to which their institutions are exposed and should receive reports that identify the size and significance of the risks in terms that are meaningful to them. In fulfilling this

responsibility, directors should take steps to develop an appropriate understanding of the risks their institutions face, possibly through briefings from auditors and experts external to the organization. Using this knowledge and information, directors should provide clear guidance regarding the level of exposures acceptable to their institutions and have the responsibility to ensure that senior management implements the procedures and controls necessary to comply with adopted policies.

Directors of institutions that conduct more traditional and less complicated business activities may require significantly less knowledge of complex financial transactions or capital markets. They may, however, be more involved in the day-to-day activities and decision-making of their institutions than are their counterparts at larger organizations and should have a level of knowledge commensurate with the nature of their involvement.

Senior management is responsible for implementing strategies in a manner that limits risks associated with each strategy and that ensures compliance with laws and regulations on both a long-term and day-to-day basis. Accordingly, management should be fully involved in the activities of their institutions and possess sufficient knowledge of all major business lines to ensure that appropriate policies, controls, and risk monitoring systems are in place and that accountability and lines of authority are clearly delineated. Senior management is also responsible for establishing and communicating a strong awareness of and need for effective internal controls and high ethical standards. Meeting these responsibilities requires senior managers of a bank or bank holding company to have a thorough understanding of banking and financial market activities and detailed knowledge of the activities their institution conducts, including the nature of internal controls necessary to limit the related risks.

In assessing the quality of the oversight by boards of directors and senior management, examiners should consider whether the institution follows policies and practices such as those described below:

- The board and senior management have identified and have a clear understanding and working knowledge of the types of risks inherent in the institution's activities and make appropriate efforts to remain informed about these risks as financial markets, risk management practices, and the institution's activities evolve.

- The board has reviewed and approved appropriate policies to limit risks inherent in the institution's lending, investing, trading, trust, fiduciary and other significant activities or products.

- The board and management are sufficiently familiar with and are using adequate record keeping and reporting systems to measure and monitor the major sources of risk to the organization.

- The board periodically reviews and approves risk exposure limits to conform with any changes in the institution's strategies, addresses new products, and reacts to changes in market conditions.

- Management ensures that its lines of business are managed and staffed by personnel with knowledge, experience, and expertise consistent with the nature and scope of the banking organization's activities.

- Management ensures that the depth of staff resources is sufficient to operate and manage soundly the institution's activities and that its employees have the integrity, ethical values, and competence that are consistent with a prudent management philosophy and operating style.

- Management at all levels provides adequate supervision of the day-to-day activities of officers and employees, including management supervision of senior officers or heads of business lines.

- Management is able to respond to risks that may arise from changes in the competitive environment or from innovations in markets in which the organization is active.

- Before embarking on new activities or introducing products new to the institution, management identifies and reviews all risks associated with the activity or product and ensures that the infrastructure and internal controls necessary to manage the related risks are in place .

**Adequate Policies, Procedures, and Limits**

An institution's directors and senior management should tailor their risk management policies and procedures to the types of risks that arise from the activities the institution conducts. Once the risks are properly identified, the institution's policies and its more fully articulated procedures provide detailed guidance for the day-to-day implementation of broad business strategies, and generally include limits designed to shield the organization from excessive and imprudent risks. While all banking organizations should have policies and procedures that address their significant activities and risks, the coverage and level of detail embodied in these statements will vary among institutions. A smaller, less complex banking organization that has effective management that is heavily involved in day-to-day operations generally would be expected to have only basic policies addressing the significant areas of operations and setting forth a limited set of requirements and procedures. In a larger institution, where senior managers must rely on widely-dispersed staffs to implement strategies in an extended range of potentially complex businesses, far more detailed policies and

related procedures would generally be expected. In either case, however, management is expected to ensure that policies and procedures address the material areas of risk to an institution and that they are modified when necessary to respond to significant changes in the banking organization's activities or business conditions.

The following guidelines should assist examiners in evaluating the adequacy of a banking organization's policies, procedures, and limits:

- The institution's policies, procedures, and limits provide for adequate identification, measurement, monitoring, and control of the risks posed by its lending, investing, trading, trust, fiduciary and other significant activities.

- The policies, procedures, and limits are consistent with management's experience level, the institution's stated goals and objectives, and the overall financial strength of the organization.

- Policies clearly delineate accountability and lines of authority across the institution's activities.

- Policies provide for the review of activities new to the financial institution to ensure that the infrastructures necessary to identify, monitor, and control risks associated with an activity are in place before the activity is initiated.

**Adequate Risk Monitoring and Management Information Systems**

Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk monitoring activities must be supported by information systems that provide senior managers and directors with timely reports on the financial condition, operating performance, and risk exposure of the consolidated organization, as well as with regular and sufficiently detailed reports for line managers engaged in the day-to-day management of the organization's activities.

The sophistication of risk monitoring and management information systems should be consistent with the complexity and diversity of the institution's operations. Accordingly, smaller and less complicated banking organizations may require only a limited set of management and board reports to support risk monitoring activities. These reports include, for example, daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report for past due loans, a simple interest rate risk report, and similar items. Larger, more complicated institutions, however, would be expected to have much more comprehensive reporting and monitoring systems that allow, for example, for more frequent reporting, tighter monitoring of complex trading activities, and the aggregation of risks on a fully

consolidated basis across all business lines and activities. Financial institutions of all sizes are expected to have risk monitoring and management information systems in place that provide directors and senior management with a clear understanding of the banking organization's positions and risk exposures.

In assessing the adequacy of an institution's measurement and monitoring of risk and its management reports and information systems, examiners should consider whether these conditions exist:

- The institution's risk monitoring practices and reports address all of its material risks.

- Key assumptions, data sources, and procedures used in measuring and monitoring risk are appropriate and adequately documented and tested for reliability on an on-going basis.

- Reports and other forms of communication are consistent with the banking organization's activities, are structured to monitor exposures and compliance with established limits, goals, or objectives, and as appropriate, compare actual versus expected performance.

- Reports to management or to the institution's directors are accurate and timely and contain sufficient information for decision-makers to identify any adverse trends and to evaluate adequately the level of risk faced by the institution.

**Adequate Internal Controls**

An institution's internal control structure is critical to the safe and sound functioning of the organization generally and to its risk management system, in particular. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties--such as trading, custodial, and back-office--is one of management's more important responsibilities.

Indeed, appropriately segregating duties is a fundamental and essential element of a sound risk management and internal control system. Failure to implement and maintain an adequate separation of duties can constitute an unsafe and unsound practice and possibly lead to serious losses or otherwise compromise the financial integrity of the institution. Serious lapses or deficiencies in internal controls, including inadequate segregation of duties, may warrant supervisory action, including formal enforcement action.

When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting, safeguards assets, and helps to ensure compliance with relevant laws, regulations, and institutional policies. Ideally, internal controls are tested by an independent internal auditor who reports directly either to the institution's board of directors or its designated committee, which is typically the audit committee. However, smaller institutions whose size and complexity do not warrant a full scale internal audit function may rely on regular reviews of essential internal controls conducted by other institution personnel. Personnel performing these reviews should generally be independent of the function they are assigned to review. Given the importance of appropriate internal controls to banking organizations of all sizes and risk profiles, the results of audits or reviews, whether conducted by an internal auditor or by other personnel, should be adequately documented, as should management's responses to them. In addition, communication channels should exist that allow negative or sensitive findings to be reported directly to the board of directors or to the relevant board committee.

In evaluating the adequacy of a financial institution's internal controls and audit procedures, examiners should consider whether these conditions are met:

- The system of internal controls is appropriate to the type and level of risks posed by the nature and scope of the organization's activities.

- The institution's organizational structure establishes clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.

- Reporting lines provide sufficient independence of the control areas from the business lines and adequate separation of duties throughout the organization--such as those relating to trading, custodial, and back-office activities.

- Official organizational structures reflect actual operating practices.

- Financial, operational, and regulatory reports are reliable, accurate, and timely; wherever applicable, exceptions are noted and promptly investigated.

- Adequate procedures exist for ensuring compliance with applicable laws and regulations.

- Internal audit or other control review practices provide for independence and objectivity.

- Internal controls and information systems are adequately tested and reviewed; the coverage, procedures, findings, and responses to audits and review tests are adequately documented; identified material weaknesses are given

appropriate and timely high level attention; and management's actions to address material weaknesses are objectively verified and reviewed.

The institution's audit committee or board of directors reviews the effectiveness of internal audits and other control review activities on a regular basis.

## RATING DEFINITIONS

The rating for risk management is based on a scale of one through five in ascending order of supervisory concern. Examiners should assign this rating to reflect findings within all four elements of sound risk management described above. The risk management rating should be reflected in the overall "Management" rating of the institution and should be consistent with the following criteria:

Rating 1 (Strong). A rating of 1 indicates that management effectively identifies and controls all major types of risk posed by the institution's activities, including those from new products and changing market conditions. The board and management are active participants in managing risk and ensure that appropriate policies and limits exist, and the board understands, reviews, and approves them. Policies and limits are supported by risk monitoring procedures, reports, and management information systems that provide management and the board with the necessary information and analysis to make timely and appropriate responses to changing conditions.

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 standards of safety and soundness and in accordance with internal and supervisory policies and practices. Risk management is considered fully effective to identify, monitor, and control risks to the institution.

Rating 2 (Satisfactory). A rating of 2 indicates that the institution's management of risk is largely effective, but lacking to some modest degree. It reflects a responsiveness and ability to cope successfully with existing and foreseeable exposures 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 being addressed. 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. Generally, risks are being controlled in a manner that does not require additional or more than normal supervisory attention.

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.

Rating 3 (Fair). A rating of 3 signifies risk management practices that 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 are considered fair, and have precluded the institution from fully addressing a significant risk 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 adequately all significant risks to the institution. Weaknesses may include continued control exceptions or failures to adhere to written policies and procedures that could have adverse effects on the institution.

The internal control system may be lacking in some important respects, particularly as indicated by continued control exceptions or by the failure to adhere to written policies and procedures. The risks associated with the internal control system could have adverse effects on the safety and soundness of the institution if corrective actions are not taken by management.

Rating 4 (Marginal). A rating of 4 represents marginal risk management practices that generally fail to identify, monitor, and control significant risk exposures in many material respects. Generally, such a situation reflects a lack of adequate guidance and supervision by management and the board. One or more of the four elements of sound risk management are considered marginal and require immediate and concerted corrective action by the board and management. A number of significant risks to the institution have not been adequately addressed, and the risk management deficiencies warrant a high degree of supervisory attention.

The institution may have serious identified weaknesses, such as an inadequate separation of duties, that require substantial improvement in its internal control or accounting procedures or in its ability to adhere to supervisory standards or requirements. Unless properly addressed, these conditions may result in unreliable financial records or reports or operating losses that could seriously affect the safety and soundness of the institution.

Rating 5 (Unsatisfactory). A rating of 5 indicates a critical absence of effective risk management practices to identify, monitor, or control significant risk exposures. One or more of the four elements of sound risk management are considered wholly deficient and management and the board have not demonstrated the capability to address deficiencies.

Internal controls may be sufficiently weak as to jeopardize seriously the continued viability of the institution. If not already evident, there is an immediate concern as to the reliability of accounting records and regulatory reports and about potential losses that could result if corrective measures are not taken immediately. Deficiencies in the institution's risk management procedures and internal controls require immediate and close supervisory attention.

## REPORTING CONCLUSIONS

For state member banks, a single numerical rating for risk management and the rationale for the rating assigned should be provided on page D, "Ratings and General Information," of the confidential section of the bank examination report. The risk management rating should also be an important factor when determining the overall management rating of the CAMEL rating system. Comments, conclusions, and criticisms relating to a bank's risk management process should be brought to the attention of management and included on the "Management/ Administration" page of the report, as well as pages 1 and 1a, "Examination Conclusions and Comments" and "Matters Requiring Board Attention" if considered appropriate. Comments in the close-out meeting with management and in the open sections of the examination report, in sufficient detail to bring about proper corrective actions, are particularly important if the examiner has assigned risk management a rating that is less than satisfactory.

Examiners should also consider the extent to which weaknesses in a bank's management of risk may indicate material noncompliance with one or more safety and soundness guidelines covering internal controls and information systems, internal audit systems, loan documentation, credit underwriting, interest rate exposure, asset growth or compensation, fees, and benefits.[1] Organizational procedures directing and enforcing an adequate separation of duties can be especially critical to some banking activities, such as so-called "front" and "back-office" functions, and should be specifically addressed by examiners. In instances in which material noncompliance is identified, authority exists to require the state member bank to submit a compliance plan within 30 days if such weaknesses are not being adequately addressed through other means.

For bank holding companies, the separate numerical rating for risk management, and the rationale for the rating assigned, should be included and discussed on page B, "Condition of Bank Holding Company," of the confidential section of the bank holding company inspection report, and should also be reflected in the examiner's overall rating of management. Comments, conclusions, and criticisms relating to an institution's risk management process should be brought to the attention

---

[1] These guidelines are included in Subpart D (Standards for Safety and Soundness) of the Board's Regulation H and became effective August 9, 1995.

of management and included on the "Policies and Supervision" page of the inspection report, as well as on page 1, "Examination Conclusions and Matters Requiring Special Board Attention" if considered appropriate and particularly if the rating is less than satisfactory.

In reports of examination or inspection and in transmittal letters to boards of directors of state member banks and bank holding companies reference should be made specifically to the types and nature of corrective actions that need to be taken by institutions to address noted risk management and internal control deficiencies. Where appropriate, institutions should also be advised that the Federal Reserve will initiate supervisory actions if the failure to separate critical operational duties creates the potential for serious losses or if material deficiencies or situations that threaten the safe and sound conduct of their activities are not adequately addressed in a timely manner. Such supervisory actions may include formal enforcement actions against the bank or bank holding company, or its responsible officers and directors, or both, and would require the immediate implementation of all necessary corrective measures.