6/8/2016

Revised February 17, 2021

Revision History: In February 2021, this guidance was revised to apply to the supervision of Federal Reserve regulated institutions with total consolidated assets of less than $100 billion including state member banks, bank holding companies, and savings and loan holding companies (including insurance and commercial savings and loan holding companies); as well as foreign banking organizations with consolidated U.S. assets of less than $100 billion. The guidance does not apply to intermediate holding companies of foreign banking organizations established pursuant to the Federal Reserve's Regulation YY with total consolidated assets of $50 billion or more. These applicability modifications align with the Board's tailoring rules. See 84 *Fed. Reg.* 59032 (November 1, 2019) for more information.

Attachment

Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion[1]

OVERVIEW

Managing risks is fundamental to the business of banking. Accordingly, the Federal Reserve places significant supervisory emphasis on an institution's management of risk, including its system of internal controls, when evaluating the overall effectiveness of an institution's risk management. An institution's failure to establish a management structure that adequately identifies, measures, monitors, and controls the risks of its activities has long been considered unsafe-and-unsound conduct. Principles of sound management should apply to the entire spectrum of risks facing an institution including, but not limited to, credit, market, liquidity, operational, compliance, and legal 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, including, but not limited to, interest rates, foreign exchange rates, commodity prices, or equity prices.
- ***Liquidity risk*** is the potential that a financial 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

[1] Supervised institutions with total consolidated assets less than $100 billion including state member banks, bank holding companies, and savings and loan holding companies (including insurance and commercial savings and loan holding companies); and foreign banking organizations (FBOs) with consolidated U.S. assets of less than $100 billion. The guidance does not apply to intermediate holding companies of foreign banking organizations established pursuant to the Federal Reserve's Regulation YY with total consolidated assets of $50 billion or more.

because of inadequate market depth or market disruptions (referred to as "market liquidity risk").

- ***Operational risk*** is the risk resulting from inadequate or failed internal processes, people, and systems or from external events.[2]
- ***Compliance risk*** is the risk of regulatory sanctions, fines, penalties or losses resulting from failure to comply with laws, rules, regulations, or other supervisory requirements applicable to a financial institution.
- ***Legal risk*** is the potential that actions against the institution that result in unenforceable contracts, lawsuits, legal sanctions, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a financial institution.

These risks and the activities associated with them are addressed in greater detail in the Federal Reserve's supervision manuals and other guidance documents.[3] In practice, an institution's business activities present various combinations, concentrations, and interrelationships of these risks depending on the nature and scope of the particular activity. The following discussion provides guidelines for the supervisory assessment of the overall effectiveness of an institution's risk management and its formal or informal systems for identifying, measuring, monitoring, and controlling these risks.

ELEMENTS OF RISK MANAGEMENT

When evaluating the risk management at an institution as part of the evaluation of the overall effectiveness of management, examiners should place primary consideration on findings relating to the following elements of a sound risk management system:

- Board[4] and senior management oversight
- Policies, procedures, and limits
- Risk monitoring and management information systems
- Internal controls

Each of these elements is described further below, along with a list of considerations relevant to assessing each element. Examiners should recognize that the considerations specified

---

[2] This definition conforms to the Basel committee's definition of operational risk.

[3] Refer to the Federal Reserve's *Commercial Bank Examination Manual*, *Bank Holding Company Supervision Manual, Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations,* and relevant FFIEC Examination Manuals.

[4] For the purpose of this guidance, for foreign banking organizations, "board of directors" refers to the equivalent governing body of the U.S. operations of the FBO.

in these guidelines are intended only to assist in the evaluation of risk management practices and are not a checklist of requirements for each institution.

An institution's risk management processes are expected to evolve in sophistication, commensurate with the institution's asset growth, complexity, and risk. At a larger or more complex organization, the institution should have more sophisticated risk management processes that address the full range of risks regardless of where the activity is conducted in the organization. Moreover, while a holding company should be able to assess the major risks of the consolidated organization, examiners should expect a parent company that centrally manages the operations and functions of its subsidiary banks to have more comprehensive, detailed, and developed risk management systems than a parent company that delegates the management of risks to relatively autonomous subsidiaries.[5]

For a small community banking organization (CBO) engaged solely in traditional banking activities and whose senior management is actively involved in the details of day-to-day operations, relatively basic risk management systems may be adequate. In accordance with the *Interagency Guidelines Establishing Standards for Safety and Soundness*, a CBO is expected, at a minimum, to have internal controls, information systems, and internal audit that are appropriate for the size of the institution and the nature, scope, and risk of its activities.[6]

The risk management processes of a regional banking organization (RBO) would typically contain detailed guidelines that set specific prudent limits on the principal types of risks relevant to a RBO's consolidated activities.[7] Furthermore, because of the diversity and the geographic dispersion of their activities, these institutions will require relatively more sophisticated information systems that provide management with timely information that supports the management of risks. The information systems, in turn, should provide management with information that present a consolidated and integrated view of risks that are relevant to the duties and responsibilities of individual managers, senior management, and the board of directors.[8]

---

[5] If these subsidiaries are regulated by another federal banking agency, Federal Reserve examiners should rely to the fullest extent possible on the conclusions drawn by relevant regulators regarding risk management. See also, SR letter 16-4, "Relying on the Work of the Regulators of the Subsidiary Insured Depository Institution(s) of Bank. Holding Companies and Savings and Loan Holding Companies with Total Consolidated Assets of Less than $100 Billion."

[6] Refer to 12 CFR 208, Appendix D-1, the *Interagency Guidelines Establishing Standards for Safety and Soundness*.

[7] As of the February 2021 revision to this guidance, the Federal Reserve generally considers an RBO to be a midsize financial institution with total consolidated assets between $10 and $100 billion.

[8] Additionally, the Federal Reserve's Regulation YY includes specific and enhanced prudential standard requirements regarding risk management for RBOs.

Consistent with the principle of national treatment,[9] the Federal Reserve has the same supervisory goals and standards for the U.S. operations of FBOs as for domestic organizations of similar size, scope, and complexity. Given the added element of foreign ownership, an FBO's risk management processes and control functions for the U.S. operations may be implemented domestically or outside of the United States. In cases where these functions are performed outside of the United States, the FBO's oversight function, policies and procedures, and information systems need to be sufficiently transparent to allow U.S. supervisors to assess their adequacy. Additionally, the FBO's U.S. senior management need to demonstrate and maintain a thorough understanding of all relevant risks affecting the U.S. operations and the associated management information systems, used to manage and monitor these risks within the U.S. operations.

The information systems at a larger institution will naturally require frequent monitoring and testing by independent control areas and by both internal and external auditors, to ensure the integrity of the information used by the board of directors and senior management in overseeing compliance with policies and limits. Therefore, an institution's risk oversight function needs to be sufficiently independent of the business lines to achieve an adequate separation of duties and the avoidance of conflicts of interest.

Board and Senior Management Oversight

The board of directors has the responsibility for establishing the level of risk that the institution should take. Accordingly, the board of directors should approve the institution's overall business strategies and significant policies, including those related to managing risks. Further, the board of directors should also ensure that senior management is fully capable of implementing the institution's business strategies and risk limits. In evaluating senior management, the board of directors should consider whether management is taking the steps necessary to identify, measure, monitor, and control these risks.

The board of directors should collectively have a balance of skills, knowledge, and experience to clearly understand the activities and risks to which the institution is exposed. The board of directors should take steps to develop an appropriate understanding of the risks the institution faces, through briefings from experts internal to their organization and potentially from external experts. The institution's management information systems should provide the board of directors with sufficient information to identify the size and significance of the risks. Using this knowledge and information, the board of directors should provide clear guidance regarding the level of exposures acceptable to the institution and oversee senior management's implementation of the procedures and controls necessary to comply with approved policies.

---

[9] National treatment requires nondiscrimination between domestic and foreign firms, or treatment of foreign entities that is no less favorable than that accorded to domestic enterprises in like circumstances. The International Banking Act of 1978 generally gives foreign banks operating in the United States the same powers as domestic banking organizations and subjects them to the same restrictions and obligations.

Senior management is responsible for implementing strategies set by the board of directors in a manner that controls risks and that complies with laws, rules, regulations, or other supervisory requirements on both a long-term and day-to-day basis. Accordingly, senior management should be fully involved in and possess sufficient knowledge of all activities 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 the need for effective risk management, internal controls, and high ethical business practices. To fulfill these responsibilities, senior management needs to have a thorough understanding of banking and financial market activities and detailed knowledge of the institution's activities, including the internal controls that are necessary to limit the related risks.

In assessing the quality of the oversight provided by the board of directors and senior management, examiners should consider the following:

- The board of directors has approved significant policies to establish risk tolerances for the institution's activities and periodically reviews risk exposure limits to align with changes in the institution's strategies, address new activities and products, and react to changes in the industry and market conditions.
- Senior management has identified and has a clear understanding and working knowledge of the risks inherent in the institution's activities. Senior management also remains informed about these risks as the institution's business activities evolve or expand and as changes and innovations occur in financial markets and risk management practices.
- Senior management has identified and reviewed risks associated with engaging in new activities or introducing new products to ensure that the necessary infrastructure and internal controls are in place to manage the related risks.
- Senior management has ensured that the institution's activities are managed and staffed by personnel with the knowledge, experience, and expertise consistent with the nature and scope of the institution's activities and risks.
- All levels of senior management provide appropriate management of the day-to-day activities of officers and employees, including oversight of senior officers or heads of business lines.
- Senior management has established and maintains effective information systems to identify, measure, monitor, and control the sources of risks to the institution.

Policies, Procedures, and Limits

Although an institution's board of directors approves an institution's overall business strategy and policy framework, senior management develops and implements the institution's risk management policies and procedures that address the types of risks arising from its activities. Once the risks are properly identified, the institution's policies and procedures should provide guidance for the day-to-day implementation of business strategies, including limits designed to prevent excessive and imprudent risks. An institution should have policies and procedures that address its significant activities and risks with the appropriate level of detail to address the type and complexity of the institution's operations. A smaller, less complex institution that has effective senior management directly involved in day-to-day operations would generally not be expected to have policies as sophisticated as larger institutions. In a larger institution, where senior managers rely on widely-dispersed staffs to implement strategies for more varied and complex businesses, far more detailed policies and procedures would generally be expected. In either case, senior management is expected to ensure that policies and procedures address the institution's material areas of risk and that policies and procedures are modified when necessary to respond to significant changes in the institution's activities or business conditions.

The following guidelines should assist examiners in evaluating an institution'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 significant risk-taking activities.
- The policies, procedures, and limits are consistent with the institution's stated strategy and risk profile.
- The policies and procedures establish accountability and lines of authority across the institution's activities.
- The policies and procedures provide for the review and approval of new business lines, products, and activities, as well as material modifications to existing activities, services, and products, to ensure that the institution has the infrastructure necessary to identify, measure, monitor, and control associated risks before engaging in a new or modified business line, product, or activity.

Risk Monitoring and Management Information Systems

Institutions of all sizes are expected to have risk monitoring and management information systems in place that provide the board of directors and senior management with timely information and a clear understanding of the institution's business activities and risk exposures. The sophistication of risk monitoring and management information systems should be commensurate with the complexity and diversity of the institution's operations. Accordingly, a smaller and less complex institution may require less frequent management and board reports to

support risk monitoring activities. For example, these reports may include, daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report on past due loans, an interest rate risk report, and similar items. In contrast, a larger, more complex institution would be expected to have much more comprehensive reporting and monitoring systems, which includes more frequent reporting to board and senior management, tighter monitoring of high-risk activities, and the ability to aggregate risks on a fully consolidated basis across all business lines, legal entities, and activities.

In assessing 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, models, and procedures used in measuring and monitoring risks are appropriate and adequately documented and tested for reliability on an on-going basis.[10]
- Reports and other forms of communication address the complexity and range of an institution's activities, monitor key exposures and compliance with established limits and strategy, and as appropriate, compare actual versus expected performance.
- Reports to the board of directors and senior management are accurate, and provide timely and sufficient information to identify any adverse trends and to evaluate the level of risks faced by the institution.

Internal Controls

An effective internal control structure is critical to the safe and sound operation of an institution. Effective internal controls promote reliable financial and regulatory reporting, safeguard assets, and help to ensure compliance with relevant laws, rules, regulations, supervisory requirements, and institutional policies. Therefore, an institution's senior management is responsible for establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate segregation of duties.

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

[10] See also SR letter 11-7, "Guidance on Model Risk Management."

Internal controls should be tested by an independent party who reports either directly to the institution's board of directors or its designated committee, which is typically the audit committee.[11] However, small CBOs 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. Given the importance of appropriate internal controls to institutions 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 the findings. In addition, communication channels should allow for adverse or sensitive findings to be reported directly to the board of directors or to the relevant board committee.

In evaluating internal controls, 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 institution's activities.
- The institution's organizational structure establishes clear lines of authority and responsibility for risk management and for monitoring adherence to policies, procedures, and limits.
- Internal audit or other control functions, such as loan review and compliance, provide for independence and objectivity.
- The official organizational structures reflect actual operating practices and management responsibilities and authority over a particular business line or activity.
- Financial, operational, risk management, and regulatory reports are reliable, accurate, and timely; and wherever applicable, material exceptions are noted and promptly investigated or remediated.
- Policies and procedures for control functions support compliance with applicable laws, rules, regulations, or other supervisory requirements.
- Internal controls and information systems are adequately tested and reviewed; the coverage, procedures, findings, and responses to audits, regulatory examinations, and other 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.

---

[11] Given the importance of the internal audit function, several additional policy statements have been issued. For comprehensive guidance on internal audit, see SR letter 03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing" and for institutions with more than $10 billion in assets, see SR letter 13-1/ CA letter 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing."

- The institution's board of directors, or audit committee, and senior management are responsible for developing and implementing an effective system of internal controls and that the internal controls are operating effectively.

Conclusions

Examiners are expected to assess risk management for an institution and assign formal ratings of "risk management" as described in the *Commercial Bank Examination Manual* for state member banks, the *Bank Holding Company Manual* for holding companies, and the *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations.*[12] In reports of examination or inspection, and in transmittal letters to the boards of directors of state member banks, holding companies,[13] and to the FBO officer of the U.S. operations, examination staff should specifically reference the types and nature of corrective actions that need to be taken by an institution to address noted risk management and internal control deficiencies. Where appropriate, the Federal Reserve will advise an institution that supervisory action will be initiated, if the institution fails to timely remediate risk management weaknesses when such failures create the potential for serious losses or if material deficiencies or situations threaten its safety and soundness. Such supervisory actions may include formal enforcement actions against the institution, or its responsible officers and directors, or both, and would require the immediate implementation of all necessary corrective measures.

If bank or holding company subsidiaries are regulated by another federal banking agency, Federal Reserve examiners should rely to the fullest extent possible on the conclusions drawn by relevant regulators regarding risk management. See also, SR letter 16-4, "Relying on the Work of the Regulators of the Subsidiary Insured Depository Institution(s) of Bank Holding Companies and Savings and Loan Holding Companies with Total Consolidated Assets of Less than $100 Billion."

---

[12] Refer to section 1000.1 of the *Commercial Bank Examination Manual*; section 1062.0 of the *Bank Holding Company Supervision Manual*; and section 2003.1 of the *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations*. For savings and loan holding companies, see also SR letter 14-9, "Incorporation of Federal Reserve Policies into the Savings and Loan Holding Company Supervision Program."

[13] This letter applies to insurance and commercial savings and loan holding companies with total consolidated assets less than $100 billion by providing core risk management guidance. Reserve Bank staff may further consult with Board staff on appropriately tailoring this guidance for these institutions.