SIDLEY
150 YEARS

JUNE 17, 2016

SIDLEY UPDATE

Federal Reserve Issues Guidance on Risk Management for Institutions With Total Consolidated Assets of Less Than $50 Billion

On June 8, 2016, the Board of Governors of the Federal Reserve System (FRB) issued supervisory letter SR 16-11, "Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets of Less than $50 Billion," with attached guidance (Guidance). The Guidance sets forth the risk management principles and supervisory expectations applicable to all FRB-supervised institutions with total consolidated assets of less than $50 billion, including bank holding companies, state member banks, savings and loan holding companies, and foreign banking organizations (FBOs) with total consolidated U.S. assets of less than $50 billion (collectively, covered institutions).

The Guidance updates and partially supersedes supervisory letter SR 95-51, "Rating the Adequacy of Risk Management and Internal Controls at State Member Banks and Bank Holding Companies."[1] In addition, the applicability of the Guidance extends to savings and loan holding companies with less than $50 billion in total consolidated assets and U.S. operations of FBOs with consolidated U.S. assets of less than $50 billion, which were not previously subject to SR 95-51.

Four elements of sound risk management are discussed in the Guidance: (1) board and senior management oversight; (2) policies, procedures and limits; (3) risk monitoring and management information systems; and (4) internal controls. The FRB will continue to issue separate guidance for individual components of risk management, such as internal audit or asset-liability management, or risk categories, such as credit or liquidity risk.

The key points of the Guidance are summarized below.

Evaluation of Risk Management

The FRB evaluates the overall effectiveness of a covered institution's risk management based on whether the covered institution adequately identifies, measures, monitors and controls its risks. A covered institution should apply sound risk management principles to its entire spectrum of risks, including but not limited to, credit risk, market risk, liquidity risk, operational risk, compliance risk and legal risk.

[1] SR 95-51 remains applicable to state member banks and bank holding companies with $50 billion or more in total consolidated assets until superseding guidance is issued for such institutions.

Risk management processes should be commensurate with a covered institution's asset growth, complexity and risk. Larger, more complex organizations are therefore expected to have more sophisticated processes that address their full range of risks. A holding company should be able to assess the major risks of the consolidated organization. However, a parent company that centrally manages the operations of its subsidiary banks is expected to have more comprehensive, detailed and developed risk management systems than a parent company that delegates risk management to relatively autonomous subsidiaries.

For FBOs with U.S. operations, the FRB applies the same risk management standards as for domestic organizations of similar size, scope and complexity, consistent with the principle of national treatment. An FBO's risk management processes and control functions for its U.S. operations may, however, be implemented domestically or outside the United States. If implemented outside the United States, the FBO's oversight function, policies and procedures, and information systems must be sufficiently transparent to allow U.S. supervisors to assess their adequacy. The FBO's U.S. senior management would also need to demonstrate a thorough understanding of all relevant risks of the U.S. operations and the associated management information systems used to manage and monitor these risks.

The Guidance notes that FRB examiners should place primary consideration on the following elements of a sound risk management system: (1) board and senior management oversight; (2) policies, procedures and limits; (3) risk monitoring and management information systems; and (4) internal controls. The considerations relevant to assessing each element set forth in the Guidance are intended to assist in the evaluation of risk management practices but should not be viewed as a checklist of requirements for each covered institution.

Board and Senior Management Oversight

Board of Directors. The board of directors at a covered institution should approve the overall business strategies and significant policies relating to risk, including established risk tolerances. The board of directors should also periodically review the risk exposure limits to ensure they address changes in strategies, new activities and products, and changes in industry and market conditions. In order to fulfill these responsibilities, the board of directors needs a collective balance of skills, knowledge and experience to clearly understand the activities and risks of the covered institution. This may require briefings from internal and external experts, and sufficient information on the size and significance of risks provided by management information systems. The board of directors should also ensure that senior management is effectively implementing the business strategies and risk limits set by the board, taking steps to identify and manage the risks, and implementing procedures and controls necessary to comply with approved policies. For FBOs, the Guidance clarifies that "board of directors" refers to the equivalent governing body of the U.S. operations of the FBO.

Senior Management. Senior management of a covered institution is responsible for implementing the strategies set by the board of directors in a manner that controls risks and complies with applicable regulatory and supervisory requirements. Senior management should therefore identify and maintain a clear understanding of the risks inherent in the institution's activities, even as business activities evolve or expand and financial markets and risk management practices change. To manage these risks, senior management should ensure that appropriate policies, controls and risk monitoring systems are in place with clearly delineated lines of authority and accountability. Other responsibilities of senior management include:

- establishing and communicating a strong awareness of the need for effective risk management, internal controls and high ethical business practices;
- identifying and reviewing risks associated with new activities or new products to ensure that the necessary infrastructure and controls are in place to manage such risks;
- ensuring that activities are managed and staffed by personnel with knowledge, experience and expertise consistent with the nature and scope of the activities and risks;
- providing appropriate management of the day-to-day activities of officers and employees, including oversight of senior officers or heads of business lines; and
- establishing and maintaining effective information systems to identify, measure, monitor and control the sources of risks.

Policies, Procedures and Limits

The senior management of a covered institution develops and implements the risk management policies and procedures for the day-to-day implementation of business strategies, including limits to prevent excessive and imprudent risks. These policies, procedures and/or limits should:

- adequately identify, measure, monitor and control the risks posed by significant risk-taking activities of the covered institution;
- address the covered institution's significant activities and material areas of risks with appropriate level of detail for the type and complexity of its operations;
- be consistent with the stated strategy and risk profile of the covered institution;
- establish accountability and lines of authority across activities;
- provide for review and approval of new or materially modified business lines, products and activities to identify, measure, monitor and control the associated risks; and
- be modified when necessary to account for significant changes in activities or business conditions.

Risk Monitoring and Management Information Systems

Covered institutions are expected to implement risk monitoring and management information systems 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 level of sophistication should be commensurate with the complexity and diversity of operations. For example, a smaller and less complex covered institution may require reports such as daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report on past due loans, an interest rating risk report and similar items. In contrast, a larger and more complex covered institution should have more comprehensive and frequent monitoring and reporting systems, 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.

A covered institution's risk monitoring practices and reports should address all material risks. Key assumptions, data sources, models and procedures used to measure risks must be appropriate, adequately documented, and

tested for reliability on an on-going basis. Reports and other forms of communication should address the complexity and range of the covered institution's activities, monitor key exposures and adherence to established limits and strategy, and as appropriate, compare actual versus expected performance. Reports must also provide accurate, timely and sufficient information on any adverse trends and the level of risks faced by the covered institution.

Internal Controls

Covered financial institutions should have in place effective internal controls to promote reliable financial and regulatory reporting to safeguard assets, and to ensure compliance with relevant regulatory and supervisory requirements and internal policies.

- The board of directors or audit committee, and senior management are responsible for development and implementing an effective system of internal controls.
- Internal controls should be appropriate for the type and level of risks posed by the covered institution's activities.
- The organizational structure should: (1) establish clear lines of authority and responsibility for risk management and for monitoring adherence to internal policies and procedures as well as adequate segregation of duties and (2) reflect actual operating practices and management responsibilities and authority over particular business lines and activities.
- Internal audit or other control functions, such as loan review and compliance, should provide for independence and objectivity.
- Financial, operational, risk management and regulatory reports should be reliable, accurate and timely and, where applicable, material exceptions should be noted and promptly investigated or remediated.
- Policies and procedures for control functions should support compliance with applicable laws, regulations and other supervisory requirements.
- Internal controls and information systems should be adequately tested by an independent party who reports either directly to the board of directors or its designated committee (typically the audit committee).
- The coverage, findings and responses to audits, regulatory examinations and other reviews should be adequately documented; identified material weaknesses must be given appropriate and timely high level attention; adverse or sensitive findings should be reported directly to the board of directors or relevant board committee; and management's corrective actions to address such weaknesses should be objectively verified and reviewed.

Risk Management Ratings

FRB examiners are expected to assess the risk management for a covered institution and assign a formal rating of "risk management" as described in the *Commercial Bank Examination Manual* for state member banks, the *Bank Holding Company Manual* for bank holding companies, and the *Examination Manual for U.S. Branches*

and Agencies for Foreign Banking Organizations for FBOs.[2] The examination reports and transmittal letters to the board of directors of state member banks, holding companies and the FBO officer of the U.S. operations should reference the types and nature of corrective actions that are required to address noted risk management and internal control deficiencies at the covered institution. Supervisory action against a covered institution and/or its responsible officers and directors may be initiated where the covered institution fails to take appropriate remedial measures and such failures create the potential for serious losses or threaten its safety and soundness.

If bank or holding company subsidiaries are regulated by another federal banking agency, the FRB will rely, to the fullest extent possible, on the conclusions drawn by such regulators regarding risk management.

Conclusion

The Guidance sets out various factors that FRB examiners and staff will consider when assessing the adequacy of a covered institution's risk management controls and deciding on the overall risk management rating. Covered financial institutions should therefore carefully evaluate their risk management governance, policies and procedures, risk identification and limits, risk monitoring and management information systems, and internal controls to ensure that they comply with the principles and supervisory expectations outlined in the Guidance and make all necessary enhancements. In particular, covered financial institutions should keep in mind that the level of sophistication and detail should be consistent with the structure, complexity, size, scope of activities and risks of the institution.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Connie M. Friesen
Partner
cfriesen@sidley.com
+1 212 839 5507

Banking and Financial Services Practice

The Banking and Financial Services Practice group offers counseling, transaction and litigation services to domestic and non-U.S. financial institutions and their holding companies, as well as securities, insurance, finance, mortgage and diversified companies that provide financial services. We also represent all sectors of the payments industry, including payment networks and processors, money transmitters, and payors and payees in various systems. We represent financial services clients before the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau and state regulatory agencies, as well as financial services regulators in other jurisdictions where we have offices. In addition, we represent clients before the United States Supreme Court, other federal courts and state courts.

[2] *See* Section A.5020 of the *Commercial Bank Examination Manual*, section 4070.1 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*.