Comptroller's Handbook

Safety and Soundness

Capital Adequacy (C) | Asset Quality (A) | **Management (M)** | Earnings (E) | Liquidity (L) | Sensitivity to Market Risk (S) | Other Activities (O)

Corporate and Risk Governance

Version 2.0, July 2019

Office of the Comptroller of the Currency

Contents

Introduction

The Office of the Comptroller of the Currency's (OCC) *Comptroller's Handbook* booklet, "Corporate and Risk Governance," is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and agencies of foreign banking organizations (collectively, banks). Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances. When it is necessary to distinguish between them, national banks[1] and federal savings associations (FSA) are referred to separately.

The general principles and practices discussed in this booklet are important protections against overarching risks to banks. This booklet

- focuses on strategic, reputation, compliance, and operational risks as they relate to governance.
- reinforces oversight of credit, liquidity, interest rate, and price risks.
- combines and updates existing national bank and FSA guidance covering the roles and responsibilities of the board of directors and senior management as well as corporate and risk governance activities and risk management practices.
- supplements other OCC and interagency guidance related to corporate and risk governance and risk management.

Other booklets in the *Comptroller's Handbook* provide detailed risk management information according to subject.

An effective corporate and risk governance framework is essential to maintaining the safe and sound operation of the bank and helping to promote public confidence in the financial system. A bank's corporate and risk governance practices should be commensurate with the bank's size, complexity, and risk profile. In accordance with the OCC's risk-based supervision approach, examiners use the core assessment in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," or "Large Bank Supervision" booklets of the *Comptroller's Handbook* when evaluating the governance of community banks, federal branches and agencies, and midsize and large banks, respectively. Expanded procedures in this and other booklets of the *Comptroller's Handbook* contain detailed guidance for examining activities or products that warrant review beyond the core assessment.

Corporate and risk governance structure and practices should keep pace with the bank's changes in size, risk profile, and complexity. Larger or more complex banks should have more sophisticated and formal board and management structures and practices.

[1] Generally, references to "national banks" throughout this booklet also apply to federal branches and agencies of foreign banking organizations unless otherwise specified. Refer to the "Federal Branches and Agencies Supervision" booklet of the *Comptroller's Handbook* for more information regarding applicability of laws, regulations, and guidance to federal branches and agencies.

Heightened Standards

Specific criteria for covered banks, subject to 12 CFR 30, appendix D, are noted in text boxes like this one throughout this booklet. 12 CFR 30, appendix D.I.E.5, "Covered Bank," describes banks subject to "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches" (heightened standards).

The assignment of the "management" rating in CAMELS[2] under the Uniform Financial Institutions Rating System is based on an assessment of the capability of the board of directors and management, in their respective roles, to identify, measure, monitor, and control the risks of a bank's activities. The rating reflects their ability to maintain the bank's safe, sound, and efficient operation in compliance with applicable laws and regulations.[3] The "management" rating reflects examiner assessments about the board and management's willingness and ability to effectively address all aspects of governance, risk management, compliance, bank operations, and financial performance. Examiners also consider Bank Secrecy Act (BSA)/anti-money laundering (AML) examination findings in a safety and soundness context when assigning the management component rating. Serious deficiencies in a bank's BSA/AML compliance program create a presumption that the bank's management component rating will be adversely affected because its risk management practices are less than satisfactory.

For purposes of this booklet, the term "board" refers to the board of directors unless otherwise stated. The board is responsible for providing effective oversight over the bank. The term "senior management" refers to bank employees designated by the board as executives responsible for making key decisions and implementing the board's vision. Senior management may include, but is not limited to, the president, chief executive officer (CEO), chief financial officer, chief risk executive (CRE),[4] chief information officer (CIO), compliance officer, chief credit officer, chief audit executive (CAE),[5] and chief bank counsel. Titles and positions vary depending on the bank's structure, size, and complexity. Unless otherwise noted, the booklet uses the terms "CEO" and "president" to refer to the individual

[2] A bank's composite rating under the Uniform Financial Institutions Rating System, or CAMELS, integrates ratings from six component areas: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk. Evaluations of the component areas take into consideration the bank's size and sophistication, the nature and complexity of its activities, and its risk profile. Federal branches and agencies are rated using the ROCA rating system, which includes the following component areas: risk management, operational controls, compliance, and asset quality.

[3] For more information about the management rating, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook*.

[4] A CRE is also commonly known as a chief risk officer.

[5] A CAE is commonly known as a chief auditor.

appointed by the board to oversee the bank's day-to-day activities. The term "management" refers to bank managers responsible for carrying out the bank's day-to-day activities, including goals established by senior management.

Corporate governance identifies the authorities and responsibilities of the board and senior management, in their respective roles, to govern the bank's operations and structure. Corporate governance involves the relationships among the bank's board, management, shareholders, and other stakeholders. Corporate governance is essential to the safe and sound operation of the bank. Corporate governance includes how the board and senior management, in their respective roles,

- set the bank's strategy, objectives, and risk appetite.
- establish the bank's risk governance framework.
- identify, measure, monitor, and control risks.
- supervise and manage the bank's business.
- protect the interests of depositors, protect the interests of shareholders or members (in the case of a mutual FSA),[6] and take into account the interests of other stakeholders.
- align corporate culture, activities, and behaviors with the expectation that the bank will operate in a safe and sound manner, operate with integrity, and comply with applicable laws and regulations.

Risk governance is an important element of corporate governance. Risk governance applies the principles of sound corporate governance to the identification, measurement, monitoring, and controlling of risks to help ensure that risk-taking activities are in line with the bank's strategic objectives and risk appetite. Risk governance is the bank's approach to risk management and includes the policies, processes, personnel, and control systems that support risk-related decision making.

Risks Associated With Corporate and Risk Governance

From a supervisory perspective, risk is the potential that events will have an adverse effect on a bank's current or projected financial condition[7] and resilience.[8] The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories are not mutually exclusive. Any product or service may expose a bank to multiple risks. Risks also may be interdependent and may be positively or negatively correlated. Examiners should be aware of and assess this interdependence. Examiners also should be alert to concentrations that can significantly elevate risk. Concentrations can accumulate within and across products,

[6] Mutual FSAs do not have shareholders. Voting rights in a mutual FSA are held by members, who are depositors (and also, in some cases, borrowers) of the association. In the context of mutual FSAs, references to "shareholders" in this booklet should be read to mean members.

[7] Financial condition includes impacts from diminished capital and liquidity. Capital in this context includes potential impacts from losses, reduced earnings, and market value of equity.

[8] Resilience recognizes the bank's ability to withstand periods of stress.

business lines, geographic areas, countries, and legal entities. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion on banking risks and their definitions. Corporate and risk governance is the framework in which all risks are managed at a bank as well as the oversight of the framework. The primary risks associated with corporate and risk governance are strategic, reputation, compliance, and operational. These risks are discussed more fully in the following paragraphs.

Strategic Risk

Strategic risk is the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment. The board and senior management, collectively, are the key decision makers that drive the strategic direction of the bank and establish governance principles. The absence of appropriate governance in the bank's decision-making process and implementation of decisions can have wide-ranging consequences. The consequences may include missed business opportunities, losses, failure to comply with laws and regulations resulting in civil money penalties (CMP), and unsafe or unsound bank operations that could lead to enforcement actions or inadequate capital.

Reputation Risk

Reputation risk is the risk to current or projected financial condition and resilience arising from negative public opinion. The strength and level of transparency of a bank's corporate and risk governance structure influence the bank's reputation with shareholders, regulators, customers, other stakeholders, and the community at large. A responsible corporate culture and a sound risk culture are the foundation of an effective corporate and risk governance framework and help form a positive public perception of the bank. A bank that fails to implement effective corporate and risk governance principles and practices may hinder the bank's competitiveness and adversely affect the bank's ability to establish new relationships and services or to continue servicing existing relationships. Departures from effective corporate and risk governance principles and practices cast doubt on the integrity of the bank's board and management. History shows that such departures can affect the entire financial services sector and the broader economy.

Compliance Risk

Compliance risk is the risk to current or projected financial condition and resilience arising from violations of laws or regulations, or from nonconformance with prescribed practices, internal bank policies and procedures, or ethical standards. Banks are subject to various laws, rules and regulations. The board is responsible for complying with applicable laws, regulations, and for understanding the legal and regulatory framework applicable to the bank's activities. The board is also responsible for meeting its fiduciary duties to the bank. Failure to establish a sound compliance program that addresses all laws and regulations, and that includes a BSA program reasonably designed to comply with the record-keeping and

reporting requirements, exposes the bank to increased legal and reputation risks and the potential for enforcement actions (including CMPs) and customer reimbursements.

Operational Risk

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events. The board oversees management's establishment and maintenance of the bank's risk management system through the risk governance framework. Sound corporate governance and risk management systems—including strategic planning, internal controls and assurance of internal controls, management information systems (MIS), and talent management—help to identify, measure, monitor, and control risks. Lapses in corporate and risk governance can increase the bank's risk profile and elevate the risk of fraud, defalcation, and other operational losses.

Corporate Governance

The board and management should be transparent about their corporate and risk governance structure and practices, with particular emphasis on board composition, the director nominating process, management succession plans, compensation, and other issues important to shareholders. The board and senior management should also play an active role in communicating with shareholders and adhering to disclosure practices. Serious errors or omissions in the bank's disclosure requirements may result in violations of law and regulation, which in turn could lead to significant regulatory penalties. The board and management should view enhanced transparency and communication as a means of building trust and public confidence that enhance the bank's value and potentially provide access to capital and funding markets.

Board's Role in Corporate Governance

The board plays a pivotal role in the effective governance of its bank. The board is accountable to shareholders, regulators, and other stakeholders. The board is responsible for overseeing management, providing organizational leadership, and establishing core corporate values. The board should create a corporate and risk governance framework to facilitate oversight and help set the bank's strategic direction, risk culture, and risk appetite. The board also oversees the talent management processes for senior management, which include development, recruiting, succession planning, and compensation.

The board should have a clear understanding of its roles and responsibilities. It should collectively have the skills and qualifications, committee structure, communication and reporting systems, and processes necessary to provide effective oversight. The board should be willing and able to act independently and provide a credible challenge to management.

The corporate and risk governance framework should provide for independent assessments of the quality, accuracy, and effectiveness of the bank's risk management functions, financial reporting, and compliance with laws and regulations. Most often performed by the bank's audit function, independent assurances are essential to the board's effective oversight of management.

The board's role in the governance of the bank is clearly distinct from management's role. The board is responsible for the overall direction and oversight of the bank—but is not responsible for managing the bank day-to-day. The board should oversee and hold management accountable for meeting strategic objectives within the bank's risk appetite. Both the board and management should ensure the bank is operating in a safe and sound manner and complying with laws and regulations.

Board Composition, Qualifications, and Selection

Board composition should facilitate effective oversight. The ideal board is well diversified and composed of individuals with a mix of knowledge and expertise in line with the bank's size, strategy, risk profile, and complexity. Although the qualifications of individual directors will vary, the directors should provide the collective expertise, experience, and perspectives necessary for effectively overseeing the bank. Boards of larger, more complex banks should include directors who have the ability to understand the organizational complexities and the risks inherent in the bank's businesses. Individual directors also should lend expertise to the board's risk oversight and compliance responsibilities. In addition, the board and its directors must meet the statutory and regulatory requirements governing size, composition, and other aspects. Refer to appendix A of this booklet for a list of these requirements.

The board should be willing and able to exercise independent judgment and provide credible challenge to management's decisions and recommendations. The board also should have an appropriate level of commitment and engagement to carry out its duties and responsibilities. To promote director independence, the board should ensure an appropriate mix of "inside" and "outside" directors. Inside directors are bank officers or other bank employees. Outside directors are not bank employees. Directors are viewed as independent if they are free of any family relationships or any material business or professional relationships (other than stock ownership and directorship itself) with the bank or its management. Independent directors bring experiences from their fields of expertise. These experiences provide perspective and objectivity because independent directors oversee bank operations and evaluate management recommendations. This mix of inside and outside directors promotes arms-length oversight. A board that is subject to excessive management influence may not be able to effectively fulfill its fiduciary and oversight responsibilities.

Generally, a director should

- be willing and able to exercise independent judgment and provide credible challenge to management's decisions and recommendations.
- have basic knowledge of the banking industry, financial regulatory system, and laws and regulations that govern the bank's operation.
- have background, knowledge, and experience in business or another discipline to facilitate bank oversight.
- accept fiduciary duties and obligations, including a firm commitment to put the bank's interests ahead of personal interests and to avoid conflicts of interest.
- have firm commitment to regularly attend and be prepared for board and committee meetings.
- have knowledge of the communities that the bank serves.

To fill board vacancies, the board should establish a process to identify, assess, and select director candidates. The bank's size and complexity may warrant the process to be written. Some boards use a nominating committee. The board or nominating committee should consider whether the director candidate has the necessary knowledge, skills, and experience in light of the bank's business and the risks presented by that business as well as sufficient

time to effectively carry out his or her responsibilities. Criteria for desired knowledge, skills, and experience may change over time if, for example, the bank plans to offer new, modified, or expanded products and services. Some boards establish additional criteria depending on certain needs. The director candidate should be willing and able to actively oversee senior management and challenge and require changes in senior management, if necessary. Additionally, inside directors should not use undue influence in selecting board members.

The board candidate should have a record of integrity in his or her personal and professional dealings, a good reputation, and a willingness to place the interests of the bank above any conflicting self-interest. The board candidate should disclose any relationships or potential conflicts of interest that the candidate or any of his or her related interests has with the bank or its affiliates. The board should consider whether a potential candidate with significant conflicts of interest that would require him or her to abstain from consideration of issues or transactions is an appropriate candidate. The bank should conduct background checks on potential board members and periodic checks of existing directors.

Diversity among directors is another important aspect of an effective board. The board should actively seek a diverse pool of candidates, including women and minorities, as well as candidates with diverse knowledge of risk management and internal controls.[9]

In most cases, nominees should be able to serve as directors immediately after they are elected in accordance with the bank's bylaws. The bank must file a prior notice with the OCC when any of the following circumstances exist:[10]

- The bank is in troubled condition, as defined by 12 CFR 5.51.
- The bank is not in compliance with minimum capital requirements as prescribed in 12 CFR 3, "Capital Adequacy Standards."
- The OCC determines, in writing, in connection with the OCC's review of a capital restoration plan under 12 USC 1831o, "Prompt Corrective Action," or otherwise, that such prior notice is appropriate.

The OCC also generally requires prior notice for new directors under additional circumstances, such as de novo banks, change in bank control, or conversions to a federal charter.[11]

[9] For more information, refer to OCC Bulletin 2015-30, "Standards for Assessing the Diversity Policies and Practices of Regulated Entities: Final Interagency Policy Statement."

[10] For more information, refer to 12 USC 1831i, "Agency Disapproval of Directors and Senior Executive Officers of Insured Depository Institutions or Depository Institution Holding Companies," and 12 CFR 5.51, "Changes in Directors and Senior Executive Officers of a National Bank or Federal Savings Association." Also, refer to the "Changes in Directors and Senior Executive Officers" and "Background Investigations" booklets of the *Comptroller's Licensing Manual*.

[11] Refer to the "Charters," "Change in Bank Control," and "Conversions to Federal Charter" booklets of the *Comptroller's Licensing Manual* for more information.

Directors should adhere to the attendance policy for regular and special board meetings. A director of a national bank may not participate or vote by proxy.[12] Excessive absences may be grounds for director dismissal. For more information, refer to the "Attend and Participate in Board and Committee Meetings" section of this booklet.

Leadership Structure of the Board

The board should determine the appropriate leadership structure. The individual selected as board chair plays a crucial leadership role in the board's proper functioning. The board chair should promote candid dialogue, encourage critical discussion, and support directors to express any dissenting views. The chair should strive to promote a well-functioning, informed, independent, and deliberative decision-making process. The chair should also have the requisite qualities, including being a respected and trusted board member, and have appropriate leadership and communication skills.

These are the two most common structures for board leadership:

- The chair is independent of the CEO.
- When the CEO and chair are the same person, the board appoints a lead director who is independent of management.

Both structures can be equally effective. When the board chair and the CEO are different individuals, however, having the separate roles may promote a more appropriate balance of power between the board and senior management.

When the board appoints a lead director in addition to a chair who also is the CEO, the board should clearly define the lead director's role. For example, a lead director typically maintains ongoing communication with the CEO, leads executive sessions of the board, works with the CEO and the board to set the board agenda, and facilitates communication between the directors and the CEO.

Outside Advisors and Advisory Directors

From time to time, the board and board committees may need to seek advice from outside advisors, who are independent of management. For example, there may be technical aspects of the bank's business—such as risk assessments, accounting matters, strategic planning, or compensation—where additional expert advice would be useful. The board should have the necessary financial resources to hire external experts to help the board fulfill its fiduciary responsibilities. Audit committees of certain banks must have members with banking or related financial management expertise, have access to their own outside counsel, and not

[12] For national banks, refer to 12 CFR 7.2009, "Quorum of the Board of Directors; Proxies Not Permissible."

include any large customers of the bank.[13] These committees may also have their own advisors.

Although qualified consultants can provide needed expertise and counsel, the board should ensure that no improper conflicts of interest exist between the bank and the consultant so that the board receives only objective and independent advice.

To leverage outside expertise, the board may consider using advisory directors. These individuals provide information and advice but do not vote as part of the board. The bank may use advisory directors in a number of situations, including

- when the operations of the bank are geographically dispersed and the board wants input from more segments of the communities served by the bank.
- when the board is small and the directors want direct involvement with a broader array of community leaders.
- to assist in business development.
- to gain access to special expertise to help the board with planning and decision making.
- to help identify likely candidates for future board openings.

Because of their limited role, advisory directors generally are not liable for board decisions. The facts and circumstances of a particular situation determine if an advisory director may have liability for individual decisions. Factors affecting potential liability include

- whether advisory directors were elected or appointed.
- how corporate documents identified advisory directors.
- the extent to which the advisory directors participated in board meetings.
- whether advisory directors exercised significant influence on the voting process.
- how the bank compensated advisory directors for attending board meetings.
- whether the advisory director had a previous relationship with the bank.

Additionally, an advisory director who, in fact, functions as a full director may be liable for board decisions in which he or she participated as if that advisory director were a full director. The OCC expects that individuals will not shield their actions from liability simply by having the word "advisory" in their titles.

Board and Board Committee Meeting Minutes

Minutes of board and board committee meetings are an essential part of the bank's records capturing the board's deliberations and actions. Board meeting minutes should be complete and accurate. Minutes should document the board's review and discussion of material action items on the agenda, any actions taken, follow-up items to be addressed at subsequent

[13] For more information, refer to 12 CFR 363.5(b), "Committees of Large Institutions." This pertains to audit committees of any bank with more than $3 billion in total assets as of the beginning of the fiscal year. Refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook* for more information on other audit committee independence considerations.

meetings, and any other issues that may arise (including approval of previous meeting minutes and board-approved policies).

Minutes should record the attendance of each director, other attendees, and directors' votes or abstentions. The record of board meetings and activities should include all materials distributed to the board for informational, oversight, or monitoring purposes. Each director should have the opportunity to review and, if appropriate, modify the minutes before the board ratifies them. Board minutes should be timely and presented for approval at the next meeting of the board. In addition, the board should receive regular reports or minutes from the various committee meetings.

The board should address the level of detail required for minutes and records of board meetings. Minutes may be subject to discovery, for example, during stockholder derivative litigation.[14] Board minutes should include sufficient information to reflect that directors were fully informed about the relevant facts, carefully deliberated the issues, provided credible challenge when necessary, and made decisions based on the best interests of the bank and its shareholders.

For stock FSAs, a director's presence at a meeting at which actions are taken on behalf of the bank is considered assenting to the action unless his or her abstention or dissent is entered in the meeting minutes.[15] A director may also file a written dissent to the action with the secretary before the meeting is adjourned or send a written dissent by registered mail to the secretary within five days after the meeting minutes are received.[16]

Access to Senior Management and Staff

Directors should have full access to all employees, if needed, but particularly senior management. Direct interaction with key staff can balance viewpoints and help ensure that information going to the board is not overly filtered. Direct interaction also can help directors deal with succession planning and management development. In addition, direct interaction with employees allows directors to assess how the corporate culture has been implemented throughout the bank. Directors can use these contacts to determine what behaviors senior managers promote.

[14] In stockholder derivative litigation, a shareholder sues both the corporation and a third party. The third party, often an executive officer or director of the corporation, is the actual defendant. The shareholder seeks recovery for the corporation from the third party.

[15] For more information, refer to 12 CFR 5.22(l)(10), "Presumption of Assent" (stock FSAs).

[16] Ibid.

Director Orientation and Training

The board should conduct orientation programs for new directors. Orientation programs vary according to bank size and complexity. At a minimum, these programs should explain

- the bank's organizational structure, corporate culture, operations, strategic plans, risk appetite, and significant issues.
- the importance of BSA/AML regulatory requirements, the ramifications of noncompliance with the BSA, and the BSA/AML risk posed to the bank.
- the individual and group responsibilities of board members, the roles of the various board committees, and the roles and responsibilities of senior management.

Directors should understand their roles and responsibilities and deepen their knowledge of the bank's business, operations, risks, and management. The board should periodically assess its skills and competencies relative to the bank's size and complexity, identify gaps, and take appropriate actions.

Management can help the board develop an ongoing education and training program to keep directors informed and current on general industry trends and regulatory developments, particularly regarding issues that pertain to their bank.

Heightened Standards

The board should establish and adhere to a formal, ongoing training program for all directors. This program should consider the directors' knowledge and experience and the covered bank's risk profile. The program should include, as appropriate, training on the following:

- Complex products, services, lines of business, and risks that have a significant impact on the covered bank.
- Laws, regulations, and supervisory requirements applicable to the covered bank.
- Other topics identified by the board.[17]

Board Compensation

Directors should be compensated fairly and appropriately. Given the demands on a director's time and the responsibilities, director compensation should be competitive and sufficient to attract and retain qualified individuals. The board or a designated committee sets and periodically reevaluates director compensation. Such compensation should be aligned with industry standards and be commensurate with an individual director's responsibilities. The board also should safeguard against payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the bank. Excessive compensation is considered an unsafe or unsound practice. Additionally, if the bank falls below required

[17] For more information, refer to 12 CFR 30, appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches"; appendix D, III; and appendix D, III.E, "Provide Ongoing Training to All Directors."

capital minimums, the compensation paid to directors should be reassessed. The reassessment may include reducing or eliminating the fees paid.

Board Tenure

A director tenure policy, though not a requirement for either public or nonpublic banks, can help the bank maintain skilled, objective, and engaged board members. A tenure policy or bylaws may, for example, establish

- director term limits.
- a mandatory retirement age.

A tenure policy can provide a road map for the board's natural evolution and create a structured process to obtain fresh ideas and promote critical thinking from new directors. A tenure policy protects against the board losing objectivity and effectiveness if long-time directors become less active, less committed, complacent, or too comfortable with the status quo. On the other hand, mandatory retirement may result in the loss of directors whose contributions to the bank continue to be valuable.

Board's Responsibilities

The board is responsible for

- providing effective oversight.
- exercising independent judgment.
- providing credible challenge to management.
- establishing an appropriate corporate culture and setting the tone at the top.
- understanding the legal and regulatory framework applicable to the bank's activities.
- complying with fiduciary duties and all applicable rules and laws.
- directing and overseeing an effective compliance management system (CMS).
- setting realistic strategic goals and objectives and overseeing management's implementation of those goals and objectives.
- confirming that the bank has a risk management system, including audit, suitable for the bank's size and activities, and understanding the bank's material risks.
- confirming that the bank has an effective system of internal controls.
- holding management accountable for implementing policies and operating within established standards and limits.
- monitoring the bank's operations, overseeing the bank's business performance, and staying informed about the bank's operating and business environment.
- selecting, retaining, and overseeing a competent CEO and senior management team.
- overseeing the compensation and benefits programs.
- setting formal performance standards for senior management, overseeing the talent management process, and approving a management succession policy for the CEO and other key executives.

- establishing and maintaining an appropriate board structure and performing board self-assessments.
- maintaining appropriate affiliate and holding company relationships.
- monitoring and supporting management's efforts to serve the convenience and needs of the communities in which the bank is chartered and its assessment area(s), including the need for credit and deposit services.[18]
- approving the bank's BSA/AML compliance program.[19]
- confirming that management's actions to correct material weaknesses, including those identified by the bank, its auditors, and regulators, are timely and effective.

Heightened Standards

Each member of a covered bank's board should oversee the covered bank's compliance with safe and sound banking practices. The board also should require management to establish and implement an effective risk governance framework that meets the minimum standards described in these guidelines. The board or the board's risk committee should approve any significant changes to the risk governance framework and monitor compliance with such framework.[20]

A covered bank's board should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may rely on risk assessments and reports prepared by independent risk management (IRM) and internal audit to support the board's ability to question, challenge, and, when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the bank.[21]

When providing active oversight under paragraph III.B of heightened standards guidelines, each member of the board should exercise sound, independent judgment.[22]

The following pages focus on some of the board's key responsibilities.

[18] Refer to 12 CFR 25, "Community Reinvestment Act and Interstate Deposit Production Regulations" (national banks) and 12 CFR 195, "Community Reinvestment" (FSAs). Also refer to OCC Bulletin 2018-17, "Community Reinvestment Act: Supervisory Policy and Processes for Community Reinvestment Act Performance Evaluations," for more information regarding CRA, including OCC supervisory policies and procedures regarding how examiners evaluate bank performance under the CRA.

[19] For more information, refer to 12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance" and the *Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

[20] For more information, refer to 12 CFR 30, appendix D, III, and appendix D, III.A, "Require an Effective Risk Governance Framework."

[21] For more information, refer to 12 CFR 30, appendix D, III, and appendix D, III.B, "Provide Active Oversight of Management."

[22] For more information, refer to 12 CFR 30, appendix D, III, and appendix D, III.C, "Exercise Independent Judgment."

Provide Oversight

The key to effective board oversight is qualified and actively involved directors. Effective board oversight can help the bank withstand economic downturns, problems with ineffective management, and other concerns. During challenging times, the board should evaluate the bank's condition, take appropriate sustainable corrective actions, and, when necessary, keep the bank operating until the board obtains capable management to fully resolve the bank's problems.

Board oversight is critical to maintaining the bank's operations in a safe and sound manner and the bank's compliance with laws and regulations. Effective board oversight includes supervising major banking activities and governing senior management. To fulfill its responsibilities, the board relies on senior management to oversee the key decisions and management to carry out the bank's day-to-day activities. The board also relies on management to provide the board with sound advice on organizational strategies, objectives, structure, and significant policies and to provide accurate and timely information about the bank's risks and financial performance. Several *Comptroller's Handbook* booklets and *The Director's Book: Role of Directors for National Banks and Federal Savings Associations* reinforce and expand on supervisory expectations regarding the board's oversight duties and management's roles and responsibilities.

Establish an Appropriate Corporate Culture

Corporate culture refers to the norms and values that drive behaviors within an organization. An appropriate corporate culture for a bank is one that does not condone or encourage imprudent risk taking, unethical behavior, or the circumvention of laws, regulations, or safe and sound policies and procedures in pursuit of profits or business objectives. An appropriate corporate culture holds employees accountable. This starts with the board, which is responsible for setting the tone at the top and overseeing management's role in fostering and maintaining a sound corporate culture and risk culture. Shared values, expectations, and objectives established by the board and senior management promote a sound corporate culture.

To promote a sound corporate culture, the board should

- establish the expectations for desired behaviors; practice and promote the expectations that all business should be conducted in a legal and ethical manner; and oversee adherence to such values by senior management and other employees.
- promote risk awareness within a sound risk culture (refer to the "Risk Culture" section for more information).
- confirm that corporate values and the code of conduct are communicated throughout the bank.
- promote clear lines of authority and accountability.
- hold management accountable for transparent and timely information.

To promote a sound corporate culture, management should

- demonstrate commitment to the corporate culture and expect the same from all employees.
- integrate the culture into the bank's strategic planning process and risk management practices.
- include desired behaviors in performance reviews and compensation practices.
- engage in continuous employee communication and training regarding risk management practices and standards of conduct.
- report and escalate material risk issues, suspected fraud, and illegal or unethical activities to the board.

Code of Ethics

The board should adopt a written code of ethics (or code of conduct) to set expected standards of behavior and professional conduct for all employees. The board should oversee management's development and periodic review of the code of ethics and other policies that address board and employee conduct, insider activities, conflicts of interest, and other relevant ethical issues. The code of ethics should encourage the timely and confidential communication of suspected fraud, misconduct, or abuse to a higher level within the bank. Such a code is intended to foster a culture of integrity and accountability.

The bank's code of ethics should address the following:

- **Conflicts of interest:** A conflict of interest occurs when an individual's private interests conflict with the bank's interests.
- **Insider activities:** Directors and executive officers should refrain from financial relationships that are or could be viewed as abusive, imprudent, or preferential. In addition, laws and regulations prohibit certain insider activities.[23]
- **Self-dealing and corporate opportunity:** Employees, officers, and directors are prohibited from using corporate property, information, or their positions for personal gain. Usurpation of a corporate opportunity is a breach of fiduciary duty.
- **Confidentiality:** All bank employees, officers, and directors must maintain the confidentiality of bank, customer, and personnel information, as required by law.
- **Fair dealing:** Employees, officers, and directors should not conceal information, abuse privileged information, misrepresent material facts, or engage in any other unfair dealing practice.
- **Protection and use of bank assets:** Company assets should be used for legitimate business purposes.
- **Compliance:** All bank employees, officers, and directors must comply with applicable laws and regulations.
- **Whistle-blower policy:** The bank should have a process for employees to report legitimate concerns about suspected illegal, unethical, or questionable practices with

[23] For more information, refer to 12 USC 1828(z), "General Prohibition on Sale of Assets"; 12 CFR 215, "Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (Regulation O)"; 12 CFR 31, "Extensions of Credit to Insiders and Transactions With Affiliates"; and the "Insider Activities" booklet of the *Comptroller's Handbook*.

protection from reprisal. This process includes the ability to escalate operational problems, inappropriate conduct, policy violations, or other risks to the bank for investigation.

- **Consequences:** Employees, officers, and directors should have a clear understanding of the consequences of unethical, illegal, or other behaviors that do not align with the bank's code of ethics (or code of conduct).

The bank should have an ethics officer, bank counsel, or some other individual from whom employees can seek advice regarding ethics questions. Ethics policies should include a process for the annual review and discussion of ethics rules at all levels of the bank, including the board. Ethics policies should be reinforced as an important part of each director's, senior manager's, and employee's performance review.

Internal audit plays an important role in monitoring the effectiveness of the bank's ethics program and whistle-blower policy. Internal audit should assess the bank's corporate culture and standards and ethics processes to identify any governance-related weaknesses. Internal audit should assure the board that suspected fraud and misconduct are promptly reported, investigated, and addressed.

Comply With Fiduciary Duties and the Law

Directors' activities are governed by common law fiduciary legal principles, which impose two duties—the duty of care and the duty of loyalty.

The duty of care requires that directors act in good faith, with the level of care that ordinarily prudent persons would exercise in similar circumstances and in a manner that the directors reasonably believe is in the bank's best interests. The duty of care requires directors to acquire sufficient knowledge of the material facts related to proposed activities or transactions, thoroughly examine all information available to them, and actively participate in decision making.

The duty of loyalty requires that directors exercise their powers in the best interests of the bank and its shareholders rather than in the directors' own self-interest or in the interests of any other person. Directors taking action on particular activities or transactions must be objective, meaning the directors must consider the activities or transactions on their merits, free from any extraneous influences. The duty of loyalty primarily relates to conflicts of interest, confidentiality, and corporate opportunity. Directors of FSAs are also subject to specific conflict of interest and corporate opportunity regulations.[24]

Each director should personally ensure that his or her conduct reflects the level of care and loyalty required of a bank director. A bank director—like the director of any corporate entity—may be held personally liable in lawsuits for losses resulting from his or her breach of fiduciary duties. Shareholders or members (either individually or on behalf of the bank),

[24] For more information, refer to 12 CFR 163.200, "Conflicts of Interest," and 12 CFR 163.201, "Corporate Opportunity."

depositors, or creditors who allege injury by a director's failure to fulfill these duties may bring these suits. In addition, the OCC may take enforcement action, including assessment of CMPs, against a director for breach of fiduciary duty.[25] The OCC may assess director liability individually because the nature of any breach of fiduciary duty can vary for each director.

Additionally, a bank director may be criminally liable for his or her actions as a director and may incur criminal liability if the director

- falsifies bank records or causes such records to be falsified.[26]
- misuses or misapplies bank funds or assets.[27]
- requests or accepts fees or gifts to influence, or as a reward for, bank business.[28]
- makes false statements generally.[29]
- commits or attempts to commit fraud.[30]
- willfully violates the BSA or its implementing regulations.[31]

Select, Retain, and Oversee Management

A profitable and sound bank is largely the result of the efforts of talented and capable management. Effective management is able to direct day-to-day operations to achieve the bank's strategic goals and objectives while operating within the risk appetite. Such management has the expertise to help the board plan for the bank's future in a changing and competitive marketplace as well as generate new and innovative ideas for board consideration. Effective management has the expertise to design and administer the systems and controls necessary to carry out the bank's strategic plan within the risk governance framework and to comply with laws and regulations.

One of the most important decisions the board makes is selecting the bank's CEO. The CEO is responsible for executing the bank's strategic plan and effectively managing the bank's risks and financial performance. The board should select and retain a CEO who has the leadership skills and the appropriate competence, experience, and integrity to carry out his or her responsibilities.

---

[25] Refer to 12 USC 1818, "Termination of Status as Insured Depository Institution."

[26] For more information, refer to 18 USC 1005, "Bank Entries, Reports, and Transactions."

[27] For more information, refer to 18 USC 656, "Theft, Embezzlement, or Misapplication by Bank Officer or Employee."

[28] For more information, refer to 18 USC 215, "Receipt of Commissions or Gifts for Procuring Loans."

[29] For more information, refer to 18 USC 1001, "Statements or Entries Generally."

[30] For more information, refer to 18 USC 1344, "Bank Fraud."

[31] For more information, refer to 31 USC 5322, "Criminal Penalties."

The board or a board committee should be actively engaged in the CEO selection process. The board should specifically define selection criteria, including experience, expertise, and personal character, and periodically review and update the criteria as appropriate. The CEO should share the board's corporate culture and the vision and philosophy for the bank to promote mutual trust and a close working relationship. For larger banks, a board committee, typically the governance or nominating committee, oversees the CEO selection process. This committee's responsibilities are discussed in more detail in appendix C of this booklet.

Besides selecting a qualified CEO, the board's primary responsibility is to directly oversee the CEO and senior management. In doing so, the board should

- set formal performance standards for senior management consistent with the bank's strategy and financial objectives, risk appetite and culture, and risk management practices; and monitor performance relative to the standards.
- align compensation with performance and ensure that incentive compensation arrangements do not encourage imprudent risk taking.
- oversee the talent management process, which includes establishing a succession plan to replace key senior management.
- approve diversity policies and practices consistent with identified standards.[32]
- meet regularly with senior management and maintain appropriate lines of communication.
- hold management accountable for providing sufficient, clear, transparent, and timely information.
- question and critically review explanations, assumptions, and information provided by senior management.
- assess whether senior management's knowledge and expertise remain appropriate given the nature and complexity of the bank's strategy and risk profile.
- take decisive action to address problems or concerns with management performance or misconduct.

Banks proposing to enter into an employment contract or other written agreement regarding compensation with a prospective director, senior executive officer, or employee may be subject to additional requirements.[33]

An FSA's board must approve any employment contract that the association enters into.[34] 12 CFR 163.39 prohibits unsafe or unsound contracts that could lead to material financial loss or damage to the association or could interfere with the board's duty or discretion to employ or terminate management or employees. For example, a contract with an excessive term could be considered unsafe or unsound. The regulation also requires that employment contracts be in writing and include certain mandatory provisions.

[32] For more information, refer to OCC Bulletin 2015-30.

[33] For more information, refer to 12 CFR 359, "Golden Parachute and Indemnification Payments."

[34] For more information, refer to 12 CFR 163.39, "Employment Contracts" (FSAs).

The board or a designated board committee should establish a formal performance appraisal process that evaluates the CEO and other senior management. The goal of a CEO evaluation process is to enhance the relationship between the CEO and the board and improve the bank's overall performance through candid conversations about goal setting and performance measurement. The board should give constructive feedback to its CEO to help improve his or her performance in overseeing the bank. This process assists the board in discharging its responsibilities to supervise management and hold the CEO accountable. When the CEO does not fulfill board expectations, the board should be prepared to replace the CEO.

Succession Planning

Succession planning can provide for stability in tumultuous financial times and can lessen the influence of dominant personalities and behaviors. At smaller banks, the depth of talent available for key management positions may be limited. In these instances, smaller banks may consider increasing the formality of management training programs, development, and talent identification. Succession planning in larger banks may involve developing a talent pool of employees who have the necessary qualifications, skills, experience, and exposure to the board and senior management. These larger banks should have more formal processes to identify management succession requirements to develop and prepare individuals for various leadership positions. The bank's succession planning may also help the bank retain key employees.

Succession planning should be a regular topic of board discussion. The board should approve a management succession policy to address the loss of the CEO and other key executives. This policy should identify critical positions that would fall in the scope of a succession plan. This policy also should outline the process by which the board and management would fill vacancies created by death, illness, injury, resignation, or misconduct. If no individual in the bank is suitable, the succession policy should provide for a temporary replacement to serve in the role until the board finds a successor. In addition, the board and senior management should review and update management succession plans at least annually to confirm that the plans remain viable.

The CEO is responsible for appropriate leadership development and management succession planning for major bank functions while effectively preserving the independence of audit and independent risk control functions. Managers should support succession planning by assessing their line-of-business structures as well as the bank's needs. Management also should determine the required knowledge and skills for management positions, identify the best candidates for critical jobs, and initiate development plans for those who show potential for advancement.

Heightened Standards

The board or board committee should review and approve a written talent management program that provides for, among other things, development, recruitment, and succession planning regarding the CEO, CAE, CRE, their direct reports, and other potential successors.[35]

Oversee Compensation and Benefits Arrangements

The board should determine that compensation practices for the bank's executive officers and employees are safe and sound, are consistent with prudent compensation practices, and comply with laws and regulations governing compensation practices.[36] For a mutual FSA or its service corporation, compensation to directors, officers, and employees should be reasonable and commensurate with their duties and responsibilities.[37] This includes former directors, officers, and employees who regularly perform services for the FSA or its service corporation under consulting contracts.

The bank is required to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the bank.[38] If it is unreasonable or disproportionate to the services actually performed, compensation is considered excessive and is therefore prohibited as an unsafe or unsound practice.[39]

Given the level of authority that executive officers have over all banking activities, the board should oversee this group's compensation, including

- evaluating and approving employment contracts.
- establishing the compensation and benefits of the CEO and other executive officers.
- assessing the reasonableness of the structure and components of executive compensation, including various benefits related to retirement, termination, and change of control.
- confirming that the internal processes for incentive compensation arrangements are consistent with safe and sound banking principles.
- evaluating executive performance relative to board-established goals and objectives.
- considering shareholder concerns.

[35] For more information, refer to 12 CFR 30, appendix D, II.L, "Talent Management Processes."

[36] For example, refer to 12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"; 12 CFR 163.39; 12 CFR 359; and 12 CFR 1026.36, "Prohibited Acts or Practices and Certain Requirements for Credit Secured by a Dwelling."

[37] For more information, refer to OCC Bulletin 2014-35, "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations."

[38] For more information, refer to 12 CFR 30, appendix A, section II, I, "Compensation, Fees and Benefits."

[39] For more information, refer to 12 CFR 30, appendix A, III, "Prohibition on Compensation That Constitutes an Unsafe and Unsound Practice."

Incentive Compensation

Incentive-based compensation means any variable compensation, fees, or benefits that serve as an incentive or reward for performance. Banks of varying size may have incentive compensation arrangements. Incentive compensation arrangements should balance risk and financial results in a manner that does not encourage employees to expose their banks to imprudent risks.

Incentive compensation can be a useful tool for retaining key talent; it may, however, encourage executives and employees to take imprudent risks that are inconsistent with the bank's long-term viability and safety and soundness. Strong corporate governance, including active and effective board oversight, should support incentive compensation arrangements.

OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies," provides guidance to all banks that have incentive compensation arrangements, with expanded expectations for the largest, most complex banks.[40] The principles in OCC Bulletin 2010-24 apply to compensation arrangements of executive officers as well as nonexecutive personnel, collectively referred to as "covered employees," who have the ability to expose the bank to material amounts of risks. OCC Bulletin 2010-24 outlines that sound incentive compensation principles should include the following:

- Provide employees with incentives that appropriately balance risk and reward.
- Be compatible with effective controls and risk management.
- Be supported by strong corporate governance, including active and effective oversight by the bank's board.

The board is ultimately responsible for ensuring that incentive compensation arrangements for all covered employees are appropriately balanced and do not jeopardize the bank's safety and soundness. The board's oversight should be commensurate with the scope and prevalence of the bank's incentive compensation arrangements. Independent directors should be actively involved in the oversight of incentive compensation arrangements.

Executive officers play a critical role in managing the overall risk-taking activities of the bank. The board should

- approve executive officers' incentive compensation arrangements.
- approve and document any material exceptions or adjustments to executive officers' incentive compensation arrangements.
- consider and monitor the effects of approved exceptions on the balance of the arrangements, the risk-taking incentives of senior executives, and the safety and soundness of the bank.
- monitor incentive compensation payments to senior executives and the sensitivity of these payments to risk results.

[40] The largest, most complex banks are those supervised by the OCC's Large Bank Supervision department.

- obtain sufficient information to monitor and review any clawback provisions to determine if the provision was triggered and executed as planned.

In larger banks, the board's oversight of compensation matters is typically handled by a board compensation committee, as discussed in appendix C of this booklet.

Employee Benefits

"Employee benefits" is an umbrella term that refers to non-wage compensation provided to employees in addition to their normal wages or salaries.

A comprehensive employee benefits package is an important, competitive, and useful tool for attracting and retaining employees. In addition, there may be tax advantages for the bank for establishing certain employee benefits, such as a retirement plan. On the other hand, offering employee benefits can be costly. Administrative costs can be high and may increase year-to-year. There is also the risk of liability from lawsuits and the payment of regulatory fines from mistakes made in benefits administration.

There are two types of employee benefits, mandated and optional. By law, banks must provide mandated benefits. The mandated benefits include Social Security, Medicare, unemployment insurance, and workers' compensation. Optional benefits are not mandated. If offered, however, optional benefits may be subject to certain requirements. If requirements are not met, the bank could incur lawsuits, penalties, and excise taxes. Optional benefits include

- group health plans.
- disability insurance.
- life insurance.
- retirement plans.
- flexible compensation (cafeteria plans).
- leave.

The board ultimately should be responsible for all decisions relating to the cost and scope of the bank's employee benefits. The board also should be responsible for overseeing management's administration of benefits and fulfillment of fiduciary responsibilities. If the board determines the bank should provide its employees with a group health plan or a retirement plan, then the board should ensure the bank's fiduciary responsibilities are met.[41]

Senior management is responsible for establishing an appropriate organizational structure to administer benefits. Management often outsources benefits administration to benefits professionals or may use an internal administrative committee or human resources department to manage some or all employee benefit operations.

[41] For more information, refer to the "Retirement Plan Products and Services" booklet of the *Comptroller's Handbook*, which contains a detailed discussion of the Employee Retirement Income Security Act of 1974 and its fiduciary standards.

Maintain Appropriate Affiliate and Holding Company Relationships

In the case of affiliated banks and holding companies, the strategic objectives, corporate values, and corporate governance principles of the affiliated bank should align with the holding company. A bank managed as part of a holding company structure can face additional challenges if directors serve on both the holding company board and the bank board. For example, this arrangement may create conflicts of interest or force directors to act on competing priorities.[42] The bank's board should ensure the interests of the bank are not subordinate to the interests of the parent holding company in decisions that may adversely affect the bank's risk profile, financial condition, safety and soundness, and compliance with laws and regulations.[43] Additionally, a director who serves on the board of both the bank and its holding company must comply with the director's fiduciary duties to the bank, including the duty of loyalty.

The primary duty of a subsidiary bank's board is to ensure the bank operates in a safe and sound manner. The subsidiary bank's board should ensure that relationships between the bank and its affiliates and subsidiaries do not pose safety and soundness issues for the bank and are appropriately managed. The bank's board should carefully review holding company policies that affect the bank to confirm that those policies adequately serve the bank. If the bank's board is concerned that the holding company is engaging in practices that may harm the bank or are otherwise inappropriate, the bank's board should notify the holding company and obtain modifications. If the holding company board does not address concerns of the bank's board, bank directors should dissent on the record and consider actions to protect the bank's interests. If necessary, the bank's board should hire an independent legal counsel or accountant. The bank's board also may raise its concerns with its regulators.

Establish and Maintain an Appropriate Board Structure

Board committees are an important component of the corporate and risk governance structure. Board committees help the board carry out oversight duties and responsibilities. Delegation of work to a committee can enhance board effectiveness by enabling the board, through its committees, to cover a wider range of issues with greater depth of analysis. Delegation also allows the directors to better focus their time and attention on areas or subject matters on which they can lend their specific expertise or experience. Committee meetings can encourage directors to thoroughly consider issues, promote more candid discussions, and gain better insight into the bank's activities.

The board should clearly understand and define the responsibilities of each committee. Each committee should have a written charter that outlines the committee's responsibilities,

[42] For more information, refer to 12 USC 371c, "Banking Affiliates"; 12 USC 371c-1, "Restrictions on Transactions with Affiliates"; 12 CFR 31; and 12 CFR 223, "Transactions Between Member Banks and Their Affiliates (Regulation W)." For more information on national banks, affiliates, and other related organizations, refer to the "Related Organizations" booklet of the *Comptroller's Handbook.* For FSAs, refer to section 730, "Related Organizations," of the *OTS Examination Handbook.*

[43] For more information, refer to the "Related Organizations" booklet of the *Comptroller's Handbook* (national banks) and section 730, "Related Organizations," of the *OTS Examination Handbook* (FSAs).

member qualifications, authorities, independence, and board reporting. The charter should establish requirements that include meeting frequency, conduct, attendance, minutes, and use of advisors. The charter also should address the need for an annual performance evaluation of the committee. The board should approve and disclose the written charter, as appropriate. Disclosure of the committee charters (for example, on websites, in proxy statements, and in policy manuals) improves the transparency of the board's decision-making processes.

The appropriate governance and committee structure depends on the bank's needs and is another key board decision. As the complexity and risk profile of the bank's products and services increase, additional committees may be necessary for the board to provide effective oversight. Similarly, additional skills and expertise of committee members might be needed. Conversely, too many committees can create competing demands and the potential for duplication and confusion about responsibilities.

Directors should be assigned to committees that align with their skills and experience. In some circumstances, directors are required to have specific qualifications to serve on certain committees.[44] Participation on multiple committees should be balanced with time commitments to avoid overburdening any single director. Some overlap, however, is beneficial in integrating board activities. With smaller boards, directors likely need to serve on multiple committees. Periodically rotating committee membership may help to achieve optimal objectivity, but frequent rotation can sometimes adversely affect the knowledge base and effectiveness of committee members. The board should find the right balance between maintaining institutional knowledge and gaining new perspectives.

The board's responsibility is to determine which committees it needs to effectively govern the bank. The committees vary by bank. Some committees are mandated by laws or regulations. Appendix C, "Common Board Committees," of this booklet describes some key committees.

Perform Board Self-Assessments

A meaningful self-assessment evaluates the board's effectiveness and functionality, board committee operations, and directors' skills and expertise. All boards should periodically undertake some form of self-assessment. Board self-assessments can be valuable in improving the board's overall performance. Further, by acknowledging that the board holds itself responsible for its performance, self-assessments help affirm the "tone at the top." The bank's directors and senior management set the tone at the top, which emphasizes personal integrity and accountability. The tone at the top also involves clearly articulating and consistently enforcing the directors' and senior management's expectations for employee behavior.

Self-assessments may take the form of questionnaires to all directors, a group self-assessment, formal interviews with each director, peer evaluations, or a combination of these

[44] For example, refer to 12 CFR 363.5, "Audit Committees," for regulatory requirements regarding the composition of audit committees for banks with consolidated total assets greater than $500 million.

methods. In some circumstances, it may be worthwhile to use an independent third party to administer the self-assessments and provide feedback to the directors.

A board self-assessment addresses the effectiveness of the board's structure, activities, and oversight, including factors such as

- director qualifications.
- level of director participation.
- quality of board meetings and discussions, including whether one director or a group of directors dominates the discussion.
- quality and timeliness of board materials and information.
- relevance and comprehensiveness of meeting agendas.
- the board's relationship with the CEO, including whether the relationship is supportive but independent.
- effectiveness of credible challenge.
- effectiveness of strategic and succession planning.
- effectiveness of executive sessions.
- effectiveness of board committees and committee structure.

An important component of any assessment is to follow up on action items identified to improve performance. The action items should produce measurable results. The board or a designated committee should oversee the implementation of recommendations arising from board self-assessments and independent assessments. As part of its oversight duties, the committee may determine that board composition changes are needed to address skill and competency gaps.

Heightened Standards

A covered bank's board should conduct an annual self-assessment that includes an evaluation of the board's effectiveness in meeting the standards applicable to the board.[45]

Oversee Financial Performance and Risk Reporting

Sound financial performance is a key indicator of the bank's success. The board is responsible for overseeing financial performance and risk reporting. As such, the board should determine the types of reports required to help with its oversight and decision-making responsibilities.[46] The reports should be accurate, timely, relevant, complete, and succinct. Refer to the "Management Information Systems" section in this booklet for more information. The information requirements, particularly the number and variety of reports, depend on the bank's size, complexity, and risks. The information should be sufficient to keep relevant parties informed of the financial condition and performance of all the bank's

[45] For more information, refer to 12 CFR 30, appendix D, III.

[46] For more information on the types of reports and measures the board uses to assist in its oversight responsibilities, refer to *Detecting Red Flags in Board Reports: A Guide for Directors*.

material lines of business. In addition, information requirements should evolve as the bank grows in size and complexity and as the bank's environment or strategic goals change.

Reports presented to the board should highlight important performance measures, trends, and variances rather than presenting the information as raw data. Some banks use dashboard-style reports to communicate the risk and performance indicators to the board.

Performance and risk reports should enable the board to

- understand the drivers of financial performance.
- understand and evaluate the potential impact of business units and their risk on financial performance.
- assess the adequacy of capital, liquidity, and earnings.
- monitor performance trends and projections.
- monitor financial performance against strategic goals.
- monitor risk positions in relation to the risk appetite, limits, and parameters.
- monitor the types, volumes, and impacts of exceptions to policies and operating procedures.
- understand model risks and reliance.
- assess the impact of new, modified, or expanded products or services.
- assess evolving risks related to changing technologies and market conditions.
- monitor risks related to third-party relationships involving critical activities.
- assess potential litigation costs and reserves.

Useful performance reports are likely to include, but are not limited to, the following information:

- Financial statements and peer comparison reports
- Budget variance reports
- Metrics on key risks
- Asset quality indicators and trends
- Allowance for loan and lease losses analysis
- Concentrations of credit
- Liquidity position and trends and contingency funding plans
- Interest rate sensitivity analyses
- Performance metrics for new, modified, or expanded products and services
- Outsourced critical activities
- Off-balance-sheet activity and exposures, including derivative exposures
- Growth rates and projections
- Capital position, trends, and capital adequacy assessments
- Key business unit performance
- Policy exception monitoring reports
- Performance measurements and metrics for risk appetite, performance goals, and strategic goals
- Earnings trends and quality, including non-interest income and expenses

Support Efforts to Serve Community Credit Needs

Banks have a responsibility to help meet the credit needs of their communities, consistent with safe and sound lending practices,[47] and an obligation to provide fair access and equal treatment to all bank customers.[48] The Community Reinvestment Act (CRA) is intended to prevent redlining and to encourage banks to help meet the credit needs of the communities they serve, including low- and moderate-income neighborhoods.[49]

The board should understand management's involvement in the community and should develop a high-level understanding of what activities meet the requirements of the CRA to ensure that strategic plans consider activities that qualify under the CRA. As part of its governance responsibilities, the board should work toward fulfilling the credit needs of the bank's community, including unmet or underserved banking needs.

Management should maintain a constructive dialogue with community members. This dialogue helps management and the board better understand where community needs are not being adequately addressed and what role the bank might play in helping to meet those needs. Significant reputation, strategic, and compliance risks and exposure to litigation exist when banks do not help meet the credit needs of their communities consistent with safe and sound lending practices or when they do not provide fair and equal treatment to all bank customers. A failure to do so can adversely affect the bank's expansion plans to acquire branches or other banks.

Individual Responsibilities of Directors

Each director has individual responsibilities and should meet these responsibilities when overseeing the bank's operations.

Attend and Participate in Board and Committee Meetings

Directors should demonstrate a willingness and ability to prepare for, attend, and participate in all board and committee meetings to make a sound contribution to the oversight function. Directors should attend meetings as often as possible. A director's time commitment should be sufficient to stay informed about the bank's risks, business and operational performance, and competitive position in the marketplace. The time commitment is generally a function of the bank's size and complexity as well as the committee work required of the director.

---

[47] Refer to 12 USC 2901 et seq., "Community Reinvestment."

[48] Refer to 15 USC 45(a)(1); 15 USC 1691(a), "Activities Constituting Discrimination"; 42 USC 3604, "Discrimination in the Sale or Rental of Housing and Other Prohibited Practices"; 42 USC 3605, "Discrimination in Residential Real Estate-Related Transactions."

[49] For more information on national banks, refer to the "Community Reinvestment Act Examination Procedures" booklet of the *Comptroller's Handbook*. For FSAs, refer to section 1500, "Community Reinvestment Act," of the *OTS Examination Handbook*.

Board meetings should be focused and productive by following agendas that permit adequate time for presentation and discussion of material issues. The thoughtful preparation of an agenda for each board meeting should provide directors with reasonable assurance that all important matters are brought to their attention. While the agenda should be carefully planned, it should be flexible enough to accommodate unexpected developments. The board should have a process for soliciting potential agenda items from individual directors and from others within the bank.

Request and Review Meeting Materials

The board should work with management to determine what information the board needs at meetings to monitor the bank's operations, make decisions, and oversee the bank's compliance with laws and regulations. Information should give directors a complete and accurate overview of the bank's condition, activities, and issues. Management is responsible for being transparent and providing information in a concise and meaningful format. Reports to the board should be subject to periodic audits to validate the integrity of the information.

Directors should be provided with information from a variety of sources, including management, board committees, outside experts and advisors, risk management and compliance personnel, and internal and external auditors. The board should agree on a set of key performance measurements and risk indicators that are tracked at each board meeting. For the board to effectively oversee the bank's adherence to the agreed-upon strategy and risk appetite, directors should have sufficient information about the bank's material risks, including emerging risks.

Directors should receive the information in advance of their meetings so there is sufficient time to review the information, reflect on key issues, prepare for discussion, and request supplemental information as necessary. The board meeting materials should be kept confidential because of the sensitive nature of the information.

The chair or lead director should periodically review the content of the meeting materials with the other directors and provide useful feedback to management. For example, instead of being inundated with technical detail, the board might request that all pre-meeting reading materials include one- to two-page executive summaries, as well as questions the directors should be prepared to address at meetings. When feasible, directors might also have access to secure online analytical tools that allow them to review additional information as needed or compare the bank's performance with a custom peer group and established benchmarks.

Make Decisions and Seek Explanations

The board's decision-making process should include constructive, credible challenge to the information and views provided by management. The ability to provide credible challenge is predicated on the qualifications of the directors and receipt of accurate, complete, and timely information. The quality of information received by the directors affects their ability to perform the board oversight function effectively. If a director is unable to make an informed decision because of inadequate information provided by management, the decision should be

postponed until sufficient information is provided and the board has additional time to discuss and review the information. If this is a recurring problem, the board should review the format of board proceedings or management's responsiveness to director inquiries. Directors should take the initiative to address potential problems.

Effective directors ask incisive questions and require accurate, timely, and honest answers. Effective directors also demonstrate a commitment to the bank, its business plan, and long-term shareholder value. In addition, they are open to other opinions and are willing to raise tough questions in a manner that encourages a constructive and engaging boardroom atmosphere.

Review and Approve Policies

Policies set standards and courses of action to achieve specific goals and objectives established by the board. The directors should approve a clear set of policies that guides management and staff in the operation and administration of the bank. The policies should cover all key areas of the bank's operations. Policies should be consistent with the bank's goals, risk appetite, and regulatory requirements. Furthermore, certain statutes and regulations require written policies governing specific activities or programs. Refer to appendix B of this booklet for a list of policies and programs subject to board approval.

The board or its designated committees should periodically review policies and oversee revisions. As appropriate, the board should approve risk limits for specific policies and monitor the limits periodically. If exceptions to a particular policy are approaching or breaching risk limits, the board should take appropriate action, which includes assessing the policy, risk appetite, or strategy. Adjustments to the strategy may include a slowdown of growth, placing a temporary moratorium on activities, or exiting the line of business. The board should modify bank policies when necessary to respond to significant changes in the bank's resources, activities, or business conditions. The board also should specify means to measure and monitor compliance with board-approved policies.

Exercise Independent Judgment

Independence is the core of effective board oversight. The board should exercise independent judgment in carrying out its responsibilities. Each director should examine and consider management's recommendations thoroughly, but exercise independent judgment. Effective credible challenge among directors is healthy and can suggest that the board is independent and not operating under undue influence by management or from an individual director.

To promote objectivity and impartiality, the bank should have a conflict of interest policy that provides clear independence standards and conflict of interest guidelines for its directors. This policy should provide sufficient guidance to address behaviors or activities that may diminish directors' ability to make objective decisions and act in the best interests of the institution. Directors should also structure their business and personal dealings with the bank to avoid even the appearance of a conflict of interest. Such dealings must comply with legal and regulatory requirements. The policy should also describe situations when directors must

abstain from decision making. Conflicts of interest should be promptly reported to the board.[50] Refer to the "Establish an Appropriate Corporate Culture" section in this booklet for more information.

To strengthen board independence, the independent directors should convene executive sessions as needed. Executive sessions allow the independent directors to discuss the effectiveness of management, the quality of board meetings, and other issues or concerns without the potential influence of management. Executive sessions make it easier for independent directors to ask questions, express unpopular opinions, and test their instincts without the risk of being seen as uninformed or undermining the CEO's authority. Executive sessions also can provide a forum for director training and meetings with advisors and regulators.

Heightened Standards

To promote effective, independent oversight of a covered bank's management, at least two members of the board

- should not be an officer or employee of the parent company or covered bank and should not have been an officer or employee of the parent company or covered bank during the previous three years.
- should not be a member of the immediate family[51] of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank.[52]
- should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the OCC's satisfaction.[53]

[50] For more information, refer to the "Insider Activities" booklet of the *Comptroller's Handbook.*

[51] As defined in 12 CFR 225.41(b)(3), "Immediate Family."

[52] As defined in 12 CFR 215.2(e)(1), "Executive Officer."

[53] Refer to 12 CFR 30, appendix D, III.D, "Include Independent Directors."

Planning

The board sets the bank's strategic focus and significant goals and provides the necessary oversight for the bank to have the personnel as well as the financial, technological, and organizational capabilities to achieve those goals. Because of ongoing changes in the banking industry, a bank should have a clear strategic plan as well as operational plans.

Strategic Planning

A strategic plan defines the bank's long-term goals and its strategy for achieving those goals. The bank should have a strategic planning process that results in a board-approved, written strategic plan. The strategic plan should be consistent with the bank's risk appetite, capital plan, and liquidity requirements.

The bank's strategic planning process should answer the following four questions for the board and senior management:

1. **Where are we now?** Senior management should evaluate the bank's internal and external environment and its strengths, weaknesses, opportunities, and threats. The internal review identifies the bank's strengths and weaknesses. The external analysis helps to recognize threats and opportunities including regulatory, economic, competitive, and technological matters.

2. **Where do we want to be?** Senior management should establish or confirm the bank's missions, goals, and objectives. A mission statement should reflect the bank's purpose and values. Goals are general statements about what should be achieved and stem from the mission and the board's vision. Objectives are statements of specific, measurable tasks that the bank, board, management, or staff needs to perform to reach its goals.

3. **How do we get there?** Senior management should design the bank's strategic plan to achieve the bank's goals and objectives. The plan should be tailored to fit the bank's internal capabilities and business environment. An effective plan should be based on realistic assumptions, consider the associated risks, and be aligned with the bank's risk appetite. The plan should take into account the resources needed to reach the bank's goals and objectives, as well as potential effect on earnings, capital, and liquidity. Technology requirements and constraints also should be considered.

4. **How do we measure our progress?** Regular measurement and reporting on the bank's objectives keep the board and senior management focused on whether the bank is achieving established goals in the strategic plan. A periodic progress report or scorecard should indicate whether timelines and objectives are being met and if additional or alternative actions need to be implemented.

As the bank grows in size and complexity and its risk profile increases, the process should become more formalized. A formalized process should define the board's and management's

roles and responsibilities, indicate timing and frequency of activities, and establish monitoring activities.

Typically, the strategic plan spans a three- to five-year period and includes the bank's goals and the objectives to achieve those goals. Strategic planning should be linked to the bank's risk management and capital planning processes. The strategic plan should be consistent with the board's articulated risk appetite and liquidity requirements as well as the bank's capital base. The strategic plan should be dynamic; as changes occur, planning and implementation should be adjusted to reflect current conditions. If the bank is a subsidiary of a holding company, the board may consider developing one consolidated strategic plan. Continuous monitoring of activities should allow management to measure the actual and potential risks associated with achieving the bank's strategic goals and objectives and the board to monitor progress. This monitoring includes whenever the bank introduces new, expanded, or modified products and services. When the bank engages in merger or acquisition activities, it should perform a retrospective review of the merger's or acquisition's success. The retrospective review should consider the impact on financial performance, information technology (IT) infrastructure, system integration, and human resources.

The board is responsible for overseeing the bank's strategic planning process and management's implementation of the resulting strategic plan. During the planning phase, the board should provide a credible challenge to management's assumptions and recommendations. The board should understand the risks associated with the success and failure of the plan. With the help of progress reports, the board should carefully monitor and assess the strategic plan. The board should ensure that management actions and decisions remain consistent with the bank's strategic plan. In addition, the board should recognize whether the bank has a reasonable strategy and, if not, challenge management's decisions, drive sustainable corrective actions, or change the strategic direction, as appropriate. The board should require management to have a contingency plan if the original plan fails to achieve its objectives.

Senior management, in consultation with the board and business line managers, should develop a strategic planning process that results in a board-approved, written strategic plan. Management is responsible for implementing the bank's strategic plan, developing policies and processes to guide the plan's execution, and monitoring the plan's implementation. Reports should include outcomes, key performance indicators, and key risk indicators that are compared with established targets and risk limits.

Heightened Standards

The CEO should be responsible for developing a written strategic plan with input from frontline units, IRM, and internal audit. The board should evaluate and approve the strategic plan and monitor management's efforts to implement the strategic plan at least annually.

The strategic plan should cover, at a minimum, a three-year period and

- contain a comprehensive assessment of risks that have an impact on the covered bank or that could have an impact on the covered bank during the period covered by the strategic plan.
- articulate an overall mission statement and strategic objectives for the covered bank, and include an explanation of how the covered bank will achieve those objectives.
- explain how the covered bank will update, as necessary, the risk governance framework to account for changes in the covered bank's risk profile projected under the strategic plan.
- be reviewed, updated, and approved, as necessary, due to changes in the covered bank's risk profile or operating environment that were not contemplated when the strategic plan was developed.[54]

New Activities

A key consideration in the bank's strategic planning process is growth and new profit opportunities for the bank. These opportunities include expanding existing products and services and introducing new ones. To stay relevant in a rapidly changing and evolving financial service industry, the bank should adapt as customer demographics, needs, and demands evolve. Remaining nimble may lead to opportunities for growth in new lines of business.

New activities, including new, modified, or expanded products and services, often require infrastructure support, expertise, substantial lead time, and significant financial investment. As such, management and the board should understand the impact of new activities on the bank's financial performance, strategic planning process, risk profile, banking model, and ability to remain competitive.[55] Insufficient planning could lead to an incomplete assessment and understanding of associated risks involved with new activities and may result in inadequate oversight and control.

The board should oversee management's implementation of the risk management system for new activities, including execution of control programs and the audit of such activities. Management should design an effective risk management system when developing and implementing new activities that includes adequate due diligence; policies, procedures, and controls; change management; and, performance and monitoring. Specifically, management should

- clearly understand the rationale for engaging in new activities and how proposed new activities meet the bank's strategic objectives.

[54] For more information, refer to 12 CFR 30, appendix D, II.D, "Strategic Plan."

[55] For more information, refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

- establish and implement policies and procedures that provide guidance on risk management of new activities.
- have effective change management processes to manage and control the implementation of new or modified operational processes, as well as the addition of new technologies into the bank's existing technology architecture.
- have appropriate performance and monitoring systems, including MIS, to assess whether the activities meet operational and strategic expectations and legal requirements and are within the bank's risk appetite.

While all banks should include these components in their risk management system for new activities, the sophistication of the risk management system should reflect the bank's size, complexity, and risk profile. The bank's risk management system should evolve to be sufficiently robust to keep pace with additional complexities and planned activities. Depending on the bank's size, complexity, and risk profile, the bank's board or management may consider establishing senior management positions or independent risk committees that include internal stakeholders from business units and other ad hoc members with expertise in applicable functions to oversee new activities.

Capital Planning

Capital planning is essential for a bank's safe and sound operations and viability.[56] Banks are expected to have capital commensurate with the nature and extent of their risks as well as their current and anticipated needs. Because raising capital normally becomes more difficult and expensive when the bank has problems, any capital raising events should begin before major issues materialize. The board and senior management should regularly assess capital to ensure that levels remain adequate, not just at one point in time, but over time.

Capital planning is a dynamic and continuous process that should be forward-looking. The capital planning process and the resulting capital plan should evolve as the bank's overall risks, activities, and risk management practices change. The most effective capital planning considers short- and long-term capital needs over at least three years. In addition, capital planning should align with the bank's strategic planning process. The content and depth of the bank's capital planning process should be commensurate with the overall risks, complexity, and corporate structure. For example, mutual savings associations build capital almost exclusively through retained earnings, so they have very limited means to increase capital quickly. Capital planning is critical for a federal mutual savings association.

Stress testing is an important element of the capital planning process. Banks can use stress testing to establish and support a reasonable risk appetite and limits, set concentration limits, adjust strategies, and appropriately plan for and maintain adequate capital levels.

[56] For more information on capital planning and stress testing, refer to the "Capital and Dividends" booklet of the *Comptroller's Handbook.*

Operational Planning

The planning process begins with developing a strategic plan. The responsibility for establishing and implementing operational plans and budgets to meet strategic plans rests with the CEO and management. Operational plans flow logically from the strategic plan by translating long-term goals into specific, measurable targets. The board should approve the operational plans after concluding that they are realistic and compatible with the bank's risk appetite and strategic objectives.

Operational plans are narrower in scope than strategic plans, have more detail, are in effect for shorter periods of time, and provide the means of monitoring progress toward achieving strategic goals. Common examples of operational plans are budgets, annual staffing, marketing, liquidity,[57] and contingency plans. The size and complexity of the bank's operations, as well as the bank's risk appetite, are important considerations when reviewing the level of formality and depth of the operational planning process.

Disaster Recovery and Business Continuity Planning

Disruptions to operations can result in loss of bank premises or systems supporting customer activities, such as online and mobile applications. Sound business continuity plans allow banks to respond to such adverse events as natural disasters, technology failures, cyber threats, human error, and terrorism. Banks should be able to restore information systems, operations, and customer services quickly and reliably after any adverse event. Banks therefore should have resilient business operations and minimize customer service disruptions.[58]

Banks' business continuity plans should forecast how departure from a business routine caused by a major operational loss could affect customer services or bank resources. Business continuity plans should address backup procedures, alternate facilities, and business resumption processes.

The board should review and approve adequate disaster recovery and business continuity plans at least annually. The board should also oversee implementation and approve policies relating to disaster recovery and business continuity. Additionally, the board should ensure management continually updates the business continuity plan to reflect the current operating environment and adequately tests the plan to confirm its viability.

Senior management is responsible for establishing and implementing policies and procedures and defining responsibilities for bank-wide business continuity planning. Management should document, maintain, and test the bank's business continuity plan and backup systems periodically to mitigate the consequences of system failures, natural and other disasters, and

[57] For more information on liquidity planning, refer to the "Liquidity" booklet of the *Comptroller's Handbook.*

[58] For more information, refer to the "Business Continuity Planning" booklet of the *FFIEC IT Examination Handbook.*

unauthorized intrusions. Management also should report the tests of the plan and backup systems to the board annually.

Information Technology and Information Security

Banks are critically dependent on their information and technology assets, such as hardware, software, and data. Management should protect information and technology assets for operational continuity, financial viability, and the trust of customers. The unauthorized loss, destruction, or disclosure of confidential information can adversely affect the bank's reputation, earnings, and capital.

Interagency guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.[59] The guidelines also discuss assigning specific responsibility for implementing an information security program and reviewing reports from management.

Based on the guidelines, the board should oversee management's development, implementation, and maintenance of a comprehensive, written information security program. The guidelines require the board or a board committee to approve the bank's written information security program at least annually.

Management should develop an information system program to protect the security and confidentiality of customer information. A robust risk assessment drives the information security program. The risk assessment provides guidance for the selection and implementation of security controls and the timing and nature of testing those controls.

Banks may employ a CIO, a chief information security officer (CISO), a chief operating officer (COO), or a chief technology officer (CTO). Titles and positions vary depending on the bank's structure, size, and complexity. This designated individual or individuals (CIO, CISO, COO, or CTO) should provide periodic updates on the bank's IT infrastructure, operations, and information security-related risks to the board.

Recovery Planning

A recovery plan's purpose is to provide a covered bank[60] with a framework to effectively and efficiently address the financial effects of severe stress events and avoid failure or resolution.[61] A recovery plan's components should generally draw from and should align with other risk management processes, such as those governing capital, liquidity, stress

[59] For more information, refer to 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards," and the "Information Security" booklet of the *FFIEC IT Examination Handbook*.

[60] "Covered Bank" is defined at 12 CFR 30, appendix E, E.3.

[61] For more information, refer to 12 CFR 30, appendix E, "OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," and the "Recovery Planning" booklet of the *Comptroller's Handbook*. Refer also to 83 Fed. Reg. 66604.

testing, business continuity, or resolution planning. An effective recovery plan helps the management of a covered bank identify when the covered bank is or may be encountering a severe stress event that threatens or may threaten its financial strength and viability. In such an event, the recovery plan should prompt management to take appropriate actions to restore the bank's financial strength and viability. The recovery plan is important to the bank's resilience, should be integrated into the bank's risk governance framework, and should play an important role in crisis management. The recovery plan should recognize the bank's transitions from business as usual to early warning of severe stress to severe stress, and it should be linked to the resolution plan in the event that financial deterioration is not rectified.

The covered bank's recovery planning process should be ongoing. The process should complement the covered bank's risk governance functions and support its safe and sound operation. The process of developing and maintaining a recovery plan should cause the covered bank's management and board to enhance their focus on risk governance with a view toward lessening the financial impact of future unforeseen events.

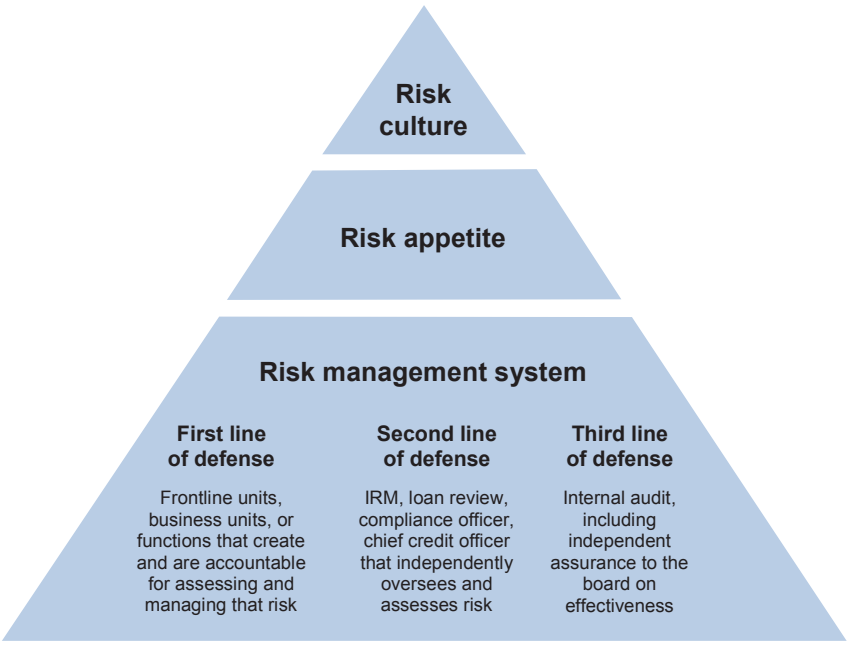
Risk Governance

Risk governance, which is part of the corporate governance framework, is the bank's approach to risk management. Risk governance applies the principles of sound corporate governance to the identification, measurement, monitoring, and controlling of risks. Risk governance helps ensure that risk-taking activities are in line with the bank's strategy and risk appetite. Key components of risk governance include the risk culture, the risk appetite, and the bank's risk management system.

A risk governance framework, as shown in figure 1, is an essential component in effectively managing the bank's enterprise-wide risks.[62] The framework is the means by which the board and management, in their respective roles,

- establish and reinforce the bank's risk culture.
- articulate and monitor adherence to the risk appetite.
- establish a risk management system with three lines of defense to identify, measure, monitor, and control risks.

Figure 1: Risk Governance Framework



The framework should cover all risk categories applicable to the bank—credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories of risk and their risk to the bank's financial condition and resilience are discussed in the "Bank Supervision Process" booklet of the *Comptroller's Handbook.* Risk governance frameworks vary among banks. Banks should have a risk governance framework commensurate with the sophistication of the bank's operations and business strategies.

[62] Refer to 12 CFR 30, appendix D.II.

Heightened Standards

A covered bank should establish and adhere to a formal written risk governance framework designed by IRM and approved by the board or the board's risk committee.[63] The risk governance framework should include delegations of authority from the board to management committees and executive officers as well as the risk limits established for material activities.[64] IRM should review and update the risk governance framework at least annually and as often as needed to address improvements in industry risk management practices and changes in the covered bank's risk profile caused by emerging risks, its strategic plans, or other internal and external factors.[65] As a general matter, a covered bank board may adopt the parent company's risk governance framework, if the parent company's framework meets the applicable regulatory standards and if the risk profiles of the parent company and covered bank are substantially the same.[66]

Risk Culture

Risk culture is the shared values, attitudes, competencies, and behaviors throughout the bank that shape and influence governance practices and risk decisions. As a subset of corporate culture, risk culture pertains to the bank's risk approach and is critical to a sound risk governance framework. To promote a sound risk culture

- the board should take the lead in establishing the tone at the top by promoting risk awareness within a sound risk culture. The board should convey its expectations to all employees that the board does not support excessive risk taking and that all employees are responsible for operating within the established risk appetite and limits.
- senior management should implement and reinforce a sound risk culture and provide incentives that reward appropriate behavior and penalize inappropriate behavior. Management should recognize, escalate, and address material risks and risk-taking activities exceeding the risk appetite in a timely manner.

Risk Appetite

The bank's risk appetite is another essential component of an effective risk governance framework and reinforces the risk culture. The bank's risk appetite is the aggregate level and types of risk that the board and management are willing to assume to achieve the bank's goals, objectives, and operating plan, consistent with applicable capital, liquidity, and other requirements. The development of a risk appetite should be driven by both top-down board leadership and bottom-up management involvement. Successful implementation depends on effective interactions among the board, senior management, IRM, and frontline units.

The board's role is to review and approve the bank's risk appetite and risk limits, including concentration limits. The risk appetite should be communicated throughout the bank. For

[63] For more information, refer to 12 CFR 30, appendix D, II.A, "Risk Governance Framework."

[64] Ibid.

[65] Ibid.

[66] For more information, refer to 12 CFR 30, appendix D, I, "Introduction."

larger, more complex banks, the board should have a written statement that outlines the risk appetite. The board should reevaluate and approve the risk appetite at least annually.

Senior management, in consultation with the board, develops the risk appetite. Senior management's responsibility is to execute the strategic, capital, and operating plans within the board-approved risk appetite and established limits. Consistent with the board-approved risk appetite, senior management should

- establish, in consultation with the board, risk limits for specific risk categories, business units, and lines of business (e.g., concentration limits).[67]
- establish appropriate metrics for measuring and monitoring risk results.
- develop timely, accurate, and transparent MIS and reports regarding risks, across the institution as well as up to the board and senior management.
- report and develop action plans, when appropriate, when limits are approached or breached.
- establish a process for material weaknesses or problems to be escalated to the appropriate level of management or the board (without fear of retribution), the CRE, and the risk committee or designated committee, as appropriate.

Heightened Standards

A covered bank should have a comprehensive written statement that articulates the bank's risk appetite and serves as the basis for the risk governance framework. The risk appetite statement provides the basis for the common understanding and communication of risk throughout the bank. The risk appetite statement should include both qualitative components and quantitative limits. The qualitative components should describe a safe and sound risk culture and how the bank will assess and accept risks, including those that are difficult to quantify. Quantitative limits should incorporate sound stress testing processes and address the bank's earnings, capital, and liquidity.[68] To be effective, the bank's risk appetite statement must be communicated and implemented throughout the bank.[69]

The board or its risk committee should review and approve the bank's risk appetite statement at least annually or more frequently, as warranted, based on the size and volatility of risks, and any material changes in the covered bank's business model, strategy, risk profile, or market conditions.[70]

The risk appetite statement should be communicated to all employees in a manner that causes all employees to align their risk-taking decisions with applicable aspects of the bank's risk appetite statement. IRM should establish and adhere to enterprise policies that include concentration risk limits. These policies should state how aggregate risks are effectively identified, measured, monitored, and controlled, consistent with the bank's risk appetite statement. Frontline units and IRM have monitoring and reporting responsibilities.[71]

[67] In smaller, less complex banks, the board, instead of senior management, may approve business line risk limits and concentrations.

[68] For more information, refer to 12 CFR 30, appendix D, II.E, "Risk Appetite Statement."

[69] For more information, refer to 12 CFR 30, appendix D, II.G, "Risk Appetite Review, Monitoring, and Communication Processes."

[70] Ibid.

[71] For more information, refer to 12 CFR 30, appendix D, II.E and II.G.

Risk Management System

The bank's risk management system comprises its policies, processes, personnel, and control systems. A sound risk management system identifies, measures, monitors, and controls risks. Because market conditions and company structures vary, no single risk management system works for all banks. The sophistication of the risk management system should be commensurate with the bank's size, complexity, and risk profile.

A common risk management system used in many banks, formally or informally, involves three lines of defense: (1) frontline units, business units, or functions that create risk; (2) IRM, loan review, compliance officer, and chief credit officer to assess risk independent of the units that create risk; and (3) internal audit, which provides independent assurance.

1. The first line of defense is the frontline units, business units, or functions that create risk. These groups are accountable for assessing and managing that risk. These groups are the bank's primary risk takers and are responsible for implementing effective internal controls and maintaining processes for identifying, assessing, controlling, and mitigating the risks associated with their activities consistent with the bank's established risk appetite and risk limits.

2. The second line of defense is commonly referred to as IRM, which oversees risk taking and assesses risks independent of the frontline units, business units, or functions that create risk. IRM complements the frontline unit's risk-taking activities through its monitoring and reporting responsibilities, including compliance with the bank's risk appetite. IRM also provides input into key risk decisions. Additionally, IRM is responsible for identifying, measuring, monitoring, and controlling aggregate and emerging risks enterprise-wide. In some banks, the second line of defense is less formal and includes such functions and roles as loan review, a compliance officer, or a chief credit officer.

3. The third line of defense is internal audit, which provides independent assurance to the board on the effectiveness of governance, risk management, and internal controls. Internal audit may be in-house, outsourced, or co-sourced.

While many banks have not formally adopted the three lines of defense, most banks have the basic elements. In smaller, noncomplex banks, risk management processes and internal controls are often integrated in the frontline units. In larger banks, the three lines of defense are more clearly defined and visible. In these banks, IRM is under the direction of a CRE or equivalent. The board or risk committee should be involved in the selection, oversight, and dismissal of the CRE. The CRE should have unfettered access to the board or board committees to discuss risk concerns identified through risk management activities.

Heightened Standards

The risk governance framework should include well-defined risk management roles and responsibilities for frontline units, IRM, and internal audit.[72] Frontline units should assess, on an ongoing basis, the material risks associated with their activities.[73] IRM should oversee the covered bank's risk-taking activities; assess risk and issues independent of frontline units; and identify and assess concentrations across the bank and material aggregate risks.[74]

Internal audit should, among other things, ensure that the covered bank's risk governance framework complies with the applicable regulatory standards and is appropriate for the bank's size, complexity, and risk profile. Internal audit should maintain a complete and current inventory of all the covered bank's material processes, product lines, services, and functions, and assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan.[75]

A covered bank's board should actively oversee the covered bank's risk-taking activities and hold management accountable for adhering to the risk governance framework. In providing active oversight, the board may rely on risk assessments and reports prepared by IRM and internal audit to support the board's ability to question, challenge, and, when necessary, oppose recommendations and decisions made by management that could cause the covered bank's risk profile to exceed its risk appetite or jeopardize the safety and soundness of the covered bank.[76]

Within a sound risk management system, the bank should have internal controls and information systems that are appropriate to the bank's size and the nature, scope, and risk of the bank's activities.[77]

Regardless of the bank's size and complexity, a sound risk management system should identify, measure, monitor, and control risk. A risk management system comprises policies, processes, personnel, and control systems. All of these elements are essential to an effective risk management system. If any of these areas are deficient, the bank's risk management may also be deficient.

To determine and confirm appropriate coverage and inform the board, management should address insurance needs as part of the bank's risk management system that identifies risk to be retained versus risk to be transferred to another party through insurance. Refer to the "Insurance" section of this booklet for more information.

[72] For more information, refer to 12 CFR 30, appendix D, II.C, "Roles and Responsibilities."

[73] For more information, refer to 12 CFR 30, appendix D, II.C.1, "Role and Responsibilities of Front Line Units."

[74] For more information, refer to 12 CFR 30, appendix D, II.C.2, "Role and Responsibilities of Independent Risk Management."

[75] For more information, refer to 12 CFR 30, appendix D, II.C.3, "Role and Responsibilities of Internal Audit."

[76] For more information, refer to 12 CFR 30, appendix D, III.B.

[77] For more information on national banks, refer to the "Internal Control" booklet of the *Comptroller's Handbook*. For FSAs, refer to section 340, "Internal Control," of the *OTS Examination Handbook.*

Identify Risk

To properly identify risks, the board and management should recognize and understand existing risks and risks that may arise from new business initiatives, including risks that originate in nonbank subsidiaries, affiliates, and third-party relationships, and those that arise from external market forces or regulatory or statutory changes. Risk identification should be a continual process and should occur at the transaction, portfolio, and enterprise levels. For larger, more complex banks, management also should identify and report to the board on the interdependencies and correlations across portfolios and lines of business that may amplify risk exposures. Proper risk identification is critical for banks undergoing mergers and consolidations to appropriately address risks. Risk identification in merging companies begins with establishing uniform definitions of risk. A common language helps with the merger's success.

Measure Risk

Accurate and timely measurement of risks is essential to effective risk management systems. A bank that does not have a risk measurement system has limited ability to control or monitor risk levels. Further, the bank needs more sophisticated measurement tools as the complexity of the risk increases. Management should periodically conduct tests to verify that the bank's measurement tools are accurate. Sound risk measurement systems assess the risks at the individual transaction, portfolio, and enterprise levels. During bank mergers and consolidations, the effectiveness of risk measurement tools is often impaired because of the incompatibility of the merging systems or other problems of integration. Consequently, management of the resulting company should make a concerted effort to confirm that risks are appropriately measured across the merged entity. Larger, more complex companies should assess the effect of increased transaction volumes across all risk categories.

Monitor Risk

Management should monitor risk levels to review risk positions and exceptions to established limits in a timely manner. Monitoring reports should be timely and accurate and should be distributed to appropriate individuals including the board to ensure action, when needed. For larger, more complex banks, monitoring is vital to confirming that management's decisions are implemented for all geographies, products and services, and legal entities. Well-designed monitoring systems allow the board to hold management accountable for operating within established risk appetites.

Control Risk

The board and management, in their respective roles, should establish and communicate risk limits through policies, standards, and procedures that define responsibility and authority. These limits should serve as a means to control exposures to the various risks associated with the bank's activities. The limits should be tools that management can adjust when conditions or risk appetites change. Management also should have a process to authorize and document exceptions to risk limits when warranted. In banks merging or consolidating, the transition

should be tightly controlled; business plans, lines of authority, and accountability should be clear. Large, diversified banks should have strong risk controls covering all geographies, products and services, and legal entities to prevent undue concentrations of risk.

The board or audit committee should require a periodic independent assessment of the bank's overall risk governance and risk management practices, which may be conducted by internal audit. The reports should provide an overall opinion on the design and effectiveness of the bank's risk governance framework, including its system of internal controls. In smaller, less complex banks, the board should consider how internal audit reviews incorporate overall risk management.

Risk Assessment Process

A risk assessment process should be part of a sound risk governance framework. A well-designed risk assessment process promotes the identification of emerging risks at an early stage and allows for the development and implementation of appropriate strategies to mitigate the risks before they have an adverse effect on the bank's safety and soundness or financial condition. The completed risk assessments should be integrated into the bank's strategic planning process and risk management activities.

The board should oversee management's implementation of the bank's risk assessment process. The board should periodically receive information about the bank's risk assessments.

Management should perform risk assessments on material bank activities at least annually, or more frequently as warranted. Completing risk assessments helps management identify current, emerging, and aggregate risks and determine if actions need to be taken to strengthen risk management. Risk assessments should measure the inherent risk, which is the risk that an activity would pose if no controls or other mitigating factors were in place. A residual risk rating should be assigned after controls are taken into account. The risk assessment process should be candid and self-critical.

Policies

Policies are statements of actions that the bank adopts to pursue certain objectives. Policies guide decisions and often set standards (on risk limits, for example) and should be consistent with the bank's underlying mission, risk appetite, and core values.

While the board or a designated board committee is responsible for approving designated policies, management is responsible for developing and implementing the policies. The CEO and management should periodically review policies for effectiveness. Policies should control the types of risks that arise from the bank's current and planned activities. To be effective, policies should clearly delineate accountability and be communicated throughout the bank.

All banks should have policies addressing their significant activities and risks. The scope and detail of those policies and procedures vary depending on bank size and complexity. A smaller, noncomplex bank whose management is heavily involved in day-to-day operations should have, at a minimum, basic policies addressing the significant areas of operations. Larger, more complex banks should have more detailed policies in which senior management relies on a widely dispersed staff to implement complex business strategies. Before introducing new activities, management should establish appropriate policies and procedures that outline the standards, responsibilities, processes, and internal controls for ensuring that risks are well understood and mitigated within reasonable parameters.

Processes

Processes are the procedures, programs, and practices that impose order on the bank's pursuit of its objectives. Processes define how activities are carried out and help manage risk. Effective processes are consistent with the underlying policies and are governed by appropriate checks and balances (such as internal controls).

Management should establish processes to implement significant bank policies. The bank's size and complexity determine the amount of detail that is needed in the policies. The design of the bank's risk management procedures, programs, and practices should be tailored to the bank's operations, activities, and business strategies and be consistent with the bank's risk appetite. Examples of bank programs include the bank's risk governance framework, audit program, CMS, and compensation program, which are discussed throughout this booklet. Refer to other booklets of the *Comptroller's Handbook* for more information about other processes for specific areas of examination.

Management is responsible for establishing a system of internal controls[78] that provides for

- an organizational structure that establishes clear lines of authority and responsibility.
- monitoring adherence to established policies.
- processes governing risk limit breaches.
- an effective risk assessment process.
- timely and accurate financial, operational, and regulatory reports.
- adequate procedures to safeguard and manage assets.
- compliance with applicable laws and regulations.

Personnel

Personnel are the bank managers and staff who execute or oversee processes. Capable management and staff are essential to effective risk management. Personnel should understand the bank's mission, risk appetite, core values, policies, and processes.

Personnel should be qualified and competent, have clearly defined responsibilities, and be held accountable for their actions. The skills and expertise of management and staff should

[78] Ibid.

be commensurate with the bank's products and services offered to customers. The skills required for larger, more complex banks are generally greater and more varied than those required in smaller, less diversified, and less complex banks. As the complexity and risk profile of the bank increase, the higher the need for qualified personnel with specific areas of expertise. Management should anticipate and assess the bank's needs and develop plans for maintaining staffing commensurate with the bank's risk profile.

Management should design programs to attract, develop, and retain qualified personnel. An effective recruitment program enhances the continuity of executive and middle management, and assists in the recruitment of individuals with the requisite skills and knowledge for various positions within the bank. Training and professional development programs are important for developing and maintaining a talent pool and further developing required skills and knowledge. For banks with limited staff or overlapping responsibilities, training and development are particularly important for continuous and consistent operations. Compensation programs should be designed to appropriately balance risk taking and reward. Management should continually assess the bank's recruitment, training and development, and compensation programs for the appropriate depth and breadth of staff.

Management should create and maintain an organizational structure with clear lines of responsibility, accountability, and oversight. Personnel in risk management and audit should have sufficient independence and stature. Position descriptions and a formal appraisal process reinforce responsibility and accountability for employees and managers. The appraisal review process provides important feedback about achieving performance goals. Effective communication promotes open dialogue, clear expectations and accountability, good decision making, and less duplication of effort.

Control Systems

Control systems are the functions (such as internal and external audits, risk review, quality control, and quality assurance) and information systems that bank managers use to measure performance, make decisions about risk, and assess the effectiveness of processes and personnel. Control functions should have clear reporting lines, sufficient resources, and appropriate access and authority. MIS should provide timely, accurate, and relevant feedback.

The effectiveness of internal controls is assessed through the bank's risk reviews (often second line of defense) and audit program (third line of defense). Risk reviews may include loan review, stress testing, compliance reviews, and back testing. Management should determine the risk reviews that should be performed in the bank. Audit programs are the independent control function that verifies the effectiveness of the bank's risk management system. Unlike risk reviews, audit managers and the board should make decisions regarding the audit program to maintain appropriate independence.

Quality Control

Quality control provides assurance that the bank consistently applies standards, complies with laws and regulations, and adheres to policies and procedures. An independent party performs the quality-control review concurrently with the bank activity. The quality-control review may be performed internally or outsourced to a third party. Quality control promotes an environment in which management and employees strive for the highest standards. An effective quality-control process significantly reduces or eliminates errors before they become systemic issues or have a negative impact on the bank's operations. Management, in consultation with the board, should determine what activities require a quality-control review, for example, secondary market mortgage loan originations, retail lending, and call center. Management also should determine the method and frequency of reporting of quality-control reviews based on regulatory requirements and risk exposure to the bank.

Quality Assurance

Quality assurance is designed to verify that established standards and processes are followed and consistently applied. An independent party performs the quality assurance review. The quality assurance review is normally performed after the bank completes the activity. Management uses the results of the quality assurance review to assess the quality of the bank's policies, procedures, programs, and practices in a specific area (for example, mortgage banking, retail lending, and internal audit). The results help management identify operational weaknesses, risks associated with the specific area, training needs, and process deficiencies. Management should determine which areas of the bank require a quality assurance review and should confirm that results of the reviews are reported to appropriate personnel.

Compliance Management System

Banking laws and regulations cover a wide range of areas, such as corporate structure, governance, bank activities, bank assets, authorities, AML, consumer protections, and political contributions.[79] Therefore, CMSs should extend beyond consumer protection laws and regulations and factor in all applicable laws and regulations as well as prudent ethical standards and contractual obligations.[80] The board and management should recognize the scope and implications of laws and regulations that apply to the bank and its activities. The board and management should understand the potential consequences of violations of laws and regulations that could result in financial losses, reputation and legal risks, and enforcement actions (including CMPs).

[79] For more information on political contributions for national banks and FSAs, refer to 52 USC 30101 et seq., "Federal Election Campaign Act of 1971," and 11 CFR 114.2, "Prohibitions on Contributions, Expenditures and Electioneering Communications." For national banks, also refer to 11 CFR 100, subpart B, "Definition of Contribution," and OCC Bulletin 2007-31, "Prohibition on Political Contributions by National Banks: Updated Guidance."

[80] For more information regarding the aspects of the bank's CMS covering consumer protection-related laws and regulations, refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook.*

The CMS should consist of the policies, procedures, and processes as well as the monitoring and testing programs that verify compliance with applicable laws and regulations and adherence to the bank's policies. All banks, regardless of size, should have a CMS that is commensurate with the risk inherent in the bank's products and services. The bank should also have monitoring in place that allows the board and management to assess the effectiveness of the bank's CMS and assists in the detection of fraud or violations of laws and regulations.

The bank's internal audit system[81] should include a periodic and independent review of the bank's CMS to provide the board and management reasonable assurance of the bank's consumer compliance-related risk management.

Many banks establish a separate compliance function headed by a compliance officer or committee. Compliance officers, or individuals in an equivalent role, should

- have a process to identify the laws and regulations applicable to the bank and its related organizations, maintain an inventory of such laws and regulations, and implement appropriate change management processes in response to new regulations or changes to regulations.[82]
- oversee the establishment of compliance monitoring and testing programs. For larger, more complex banks, this testing occurs in a second-line function that is independent of the business units.
- establish reporting processes in an effort to provide relevant information to appropriate parties.
- develop reports and metrics to monitor performance.
- implement and oversee compliance-related training programs for all employees and directors. Proper training programs reflect subject matter, depth, and frequency appropriate to job responsibilities. Escalation and reporting procedures should be in place for employees who do not complete the required training.

The board should oversee the bank's CMS. For larger, more complex banks, the board should receive periodic reports on the bank's state of compliance. The board is responsible for establishing a culture that places a high priority on compliance and holds management accountable.

Management should establish and clearly communicate compliance roles, responsibilities, and expectations that compliance with all laws and regulations is an organizational priority for all employees. Management is responsible for the timely correction of deficiencies found by compliance personnel, risk managers, internal and external auditors, and regulators. Management is responsible for implementing processes that promptly escalate material issues

[81] Refer to 12 CFR 30, appendix A, II.A, "Operational and Managerial Standards," and the "Internal and External Audits" booklet of the *Comptroller's Handbook* for information regarding internal audit systems, including compliance audit systems.

[82] The designation of responsibility over the change management process is a senior management decision and may vary from bank to bank.

to senior management and the board. Management also should implement and maintain a mechanism for employees to confidentially raise concerns about illegal activities, violations, and nonadherence to bank policies.

Bank Secrecy Act/Anti-Money Laundering Program

The BSA is intended to safeguard the U.S. financial system and the banks that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. The BSA requires banks to establish a BSA/AML compliance program to fulfill its record-keeping and reporting requirements and to confirm the identity of bank customers.[83] The board is responsible for approving and overseeing management's implementation of the BSA/AML compliance program. The program must include[84]

- a system of internal controls to ensure ongoing compliance.
- independent testing of BSA/AML compliance.
- a designated individual or individuals responsible for managing BSA compliance (BSA compliance officer).
- training for appropriate personnel.
- a customer identification program.[85]

The program should also contain appropriate risk-based procedures for conducting ongoing customer due diligence, including[86]

- understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile.
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[87]

Senior management should communicate and reinforce the BSA/AML compliance culture established by the board. Senior management is also responsible for implementing and enforcing the board-approved BSA/AML compliance program.[88]

---

[83] For more information, refer to the *FFIEC BSA/AML Examination Manual.*

[84] For more information, refer to 12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act Compliance."

[85] For more information, refer to 12 CFR 21.21(c)(2), "Customer Identification Program."

[86] For more information, refer to 31 CFR 1020.210, "Anti-Money Laundering Program Requirements for Financial Institutions Regulated Only by a Federal Functional Regulator, Including Banks, Savings Associations, and Credit Unions."

[87] Ibid.

[88] Refer to 12 CFR 21.21(c) "Establishment of a BSA Compliance Program," and 12 CFR 21.21(d)(3).

Audit Program

Well-planned, properly structured audit programs are essential to effective risk management and internal control systems and are also a critical defense against fraud.[89] The audit program consists of an internal audit function and an external audit function. An internal audit program provides assurance to the board and senior management not only on the quality of the bank's internal controls but also on the effectiveness of risk management, financial reporting, MIS, and governance practices. Internal auditors should be independent of the audited activities and have sufficient stature, authority, and board support to carry out their assignments with objectivity. The external audit function complements the internal audit function by providing management and the board with an independent and objective view of the reliability of the bank's financial statements and the adequacy of its system of internal controls over the bank's financial statements. When a third party provides both audit and consulting services, special care should be taken to preserve audit independence. Specifically, the firm should not audit the activities for which it provided consultation services.[90]

The board may delegate the design, implementation, and monitoring of the system of internal controls to management and delegate the testing and assessment of internal controls to internal auditors or other external third parties. Establishing an independent audit committee to oversee and maintain the audit functions is a good, and sometimes required, practice.[91] See appendix C, "Common Board Committees," of this booklet for more information on audit committee responsibilities. The board and senior management are responsible for having an effective system of internal controls and an effective audit system in place.[92]

The chief auditor is the person assigned responsibility for the internal audit function.[93] The chief auditor reports directly to the audit committee or the board in the absence of the audit committee. The OCC expects the chief auditor to be a bank employee, but the chief auditor may have dual reporting relationships. The objectivity of internal audit is best served when the chief auditor is functionally accountable to the audit committee but reports administratively to the CEO. The chief auditor may also be a dual employee of the holding

[89] For more information on effective audit functions, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook.*

[90] For more information, refer to OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing."

[91] 12 CFR 363.5(a), "Composition and Duties," requires insured banks with $500 million or more in total assets to have a dedicated audit committee. 12 CFR 363, appendix A.27, "Composition," outlines audit committee requirements as they should be applied to banks and insured branches of foreign banks. Refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook* for more information on audit committees.

[92] Refer to 12 CFR 30, appendix A, II.A. Internal control systems include internal controls and information systems.

[93] Refer to OCC Bulletin 2003-12. In small banks that do not have a formal internal or external audit program, internal audit responsibilities may lie with an officer or employee. Refer the "Internal and External Audits" booklet of the *Comptroller's Handbook* for more information.

company. The chief auditor implements the audit program and reports audit activities to the audit committee. The chief auditor should have the appropriate stature and authority in the bank to perform his or her duties, and, in certain larger banks, regulation requires the position rest one level below the CEO.[94] When the bank outsources the internal audit activities, the board and senior management should designate an audit liaison to coordinate audit activities.

Heightened Standards

The audit committee reviews and approves internal audit's overall charter and audit plans. The audit committee should approve all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The committee may oversee the CAE's administrative activities or designate them to the CEO.[95]

The heightened standards impose additional requirements on audit plans, as well as additional circumstances in which the internal audit should make reports to the audit committee. The audit committee should be aware of and monitor the internal audit's compliance with these heightened standards.[96]

Management Information Systems

Banks rely heavily on IT to process bank transactions, maintain critical records, and supply reports to the board and management about managing business risk.[97] As such, a bank's IT systems should have the capability to aggregate risks across the bank in a timely manner and under stress situations. Information provided by management in reports should be accurate, timely, and sufficiently detailed to oversee the bank's safe and sound operation.

MIS broadly refers to a comprehensive process, supported by computer-based systems, that provides the information necessary to manage the bank. To function effectively as an interactive, interrelated, and interdependent feedback system for management and staff, MIS should be useable. The five elements of a useable MIS are timeliness, accuracy, consistency, completeness, and relevance. The effectiveness of MIS is hindered whenever one or more of these elements is compromised.

Timeliness: To simplify prompt decision making, the bank's MIS should be capable of providing and distributing current information to appropriate users. Information systems should be designed to expedite reporting of information. The system should be able to quickly collect and edit data, summarize results, and adjust and correct errors.

Accuracy: A sound system of automated and manual internal controls should exist throughout all information systems processing activities. Information should receive appropriate editing, balancing, and internal control checks. The bank should employ a

[94] Refer to 12 CFR 30, appendix D, I.E.2, "Chief Audit Executive."

[95] For more information, refer to 12 CFR 30, appendix D, I.E.8, "Internal Audit."

[96] For more information, refer to 12 CFR 30, appendix D, II.C.3.

[97] For more information, refer to the "Management" booklet of the *FFIEC IT Examination Handbook*.

comprehensive internal and external audit program to validate the adequacy of internal controls.

Consistency: To be reliable, data should be processed and compiled consistently and uniformly. Variations in how the bank collects and reports data can distort information and trend analysis. In addition, because data collection and reporting processes change over time, management should establish sound procedures to allow for systems changes. These procedures should be well defined and documented, be clearly communicated to appropriate employees, and include an effective monitoring system.

Completeness: Decision makers need complete and pertinent information in summarized form. Management should capture and aggregate all of the bank's material risk exposures, including those that are off-balance-sheet. Data should be available by groupings, such as by business line, asset type, and industry, that are relevant for the risk in question. Also, the data groupings should allow for the identification and reporting on risk exposures, concentrations, and emerging risks.

Relevance: Information provided to management should be relevant. Information that is inappropriate, unnecessary, or too detailed for effective decision making has no value. MIS should be appropriate to support the management level using the information. The relevance and level of detail provided through MIS should directly correlate to the needs of the board, senior management, departmental or area mid-level managers, and others in the performance of their jobs.

MIS do not necessarily reduce expenses. Development of meaningful systems and their proper use lessen the probability that erroneous decisions will be made because of inaccurate or untimely information. Erroneous decisions invariably misallocate or waste resources, which may adversely affect earnings or capital.

Heightened Standards

The risk governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for the following:

- The design, implementation, and maintenance of a data architecture and IT infrastructure that support the covered bank's risk aggregation and reporting needs during both normal times and times of stress.
- The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board and the OCC.[98]
- The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.[99]

[98] For more information, refer to 12 CFR 30, appendix D, II.J, "Risk Data Aggregation and Reporting."

[99] For more information, refer to the Basel Committee on Banking Supervision's "Principles for Effective Risk Data Aggregation and Risk Reporting," January 2013.

Third-Party Risk Management

Banks increasingly rely on third-party relationships to provide technological, administrative, and operational services on the bank's behalf. The bank's use of third parties does not diminish the board and senior management's responsibility to ensure that the activity is performed in a safe and sound manner and complies with applicable laws and regulations.

Management should adopt third-party risk management processes commensurate with the level of risk and complexity of the bank's third-party relationships and organizational structure.[100] The board and management should provide more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities.

Management should adopt a third-party risk management process that follows a continuous life cycle for all relationships and incorporates planning, due diligence, and third-party selection, contract negotiation, ongoing monitoring, and termination.

Insurance

The board should be responsible for the adequacy of insurance coverage and other insurance needs. As part of an effective risk management system, the board should determine the uninsured loss the bank is able and willing to assume. Management can implement additional controls to minimize and retain risk. Management may transfer the risk to another party through insurance or contractual transfer, self-insure the risk, or use any combination of these options. A basic tenet of risk management is that risks carrying the potential for catastrophic or significant loss should not be retained. Conversely, it typically is not cost-justified to insure losses that are relatively predictable and not severe. Teller drawer shortages are an example. It would be less costly to improve controls or training procedures intended to reduce those shortages than to pay additional insurance premiums to cover the losses.

The board should determine the maximum loss the bank is able and willing to assume. Once the decision is made to insure a particular risk, a knowledgeable, professional insurance agent can help with selecting an underwriter. Management should assess the financial capacity of the insurance underwriter to determine that the company has the ability to make payment should a significant loss occur. Additionally, the board and management should review the bank's insurance annually.

Appendix D of this booklet explains major types of insurance coverage available to banks.

[100] For more information, refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"; OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"; and the "Outsourcing Technology Services" booklet of the *FFIEC IT Examination Handbook.*

Insurance Record Keeping

The breadth of available insurance policies and differences in the coverage emphasize the importance of maintaining a concise, easily referenced schedule of insurance coverage. These records should include the

- coverage provided, detailing major exclusions.
- underwriter.
- deductible amount.
- upper limit.
- term of the policy.
- date premiums are due.
- premium amount.

Records of losses also should be maintained and included whether or not the bank was reimbursed. These records indicate where internal controls may need to be improved and are useful in measuring the level of risk exposure in a particular area.

Board and Management's Roles in Risk Governance

The board or risk committee and senior management play critical roles in the bank's risk governance by (1) setting the tone at the top, (2) setting the bank's strategic objectives and risk appetite, and (3) establishing an appropriate risk management system to manage the risks associated with meeting the strategic objectives.

Risks may arise from bank activities or activities of subsidiaries, affiliates, counterparties, or third-party relationships. Any product, service, or activity may expose the bank to multiple risks. These risks may be interdependent—an increase in one category of risk may cause an increase in others. Because of the interrelationship of the bank's risks and the potential impact on its earnings, capital, and strategic objectives, the risks should be assessed, evaluated, and managed enterprise-wide. This concept is commonly referred to as enterprise risk management (ERM). ERM helps the board and management view the bank's risks in a comprehensive and integrated manner. ERM also helps identify concentrations that may arise across multiple business lines that, when aggregated, represent concentration risk that may require board attention and management actions. To be successful, ERM should be supported by the board and senior management. If the bank is a subsidiary of a holding company, it may be appropriate to implement ERM corporate-wide.

Board's Responsibilities

The board should oversee the design and implementation of the risk governance framework. The board should require periodic independent assessments to determine the framework's effectiveness.

The board should oversee the bank's risk management system to confirm that the system identifies, measures, monitors, and controls risks. If the bank does not have a CRE, the board

should appoint a qualified individual or committee to oversee the bank's ERM process. While a qualified individual independent of day-to-day frontline management is preferred, it may not be practical for every bank. When impractical, the board should consider selecting a senior-level staff member who has a good understanding of the bank's operations across the various business lines. This person should have access to the board or risk committee to convey risk concerns.

The board should oversee the bank's compliance management programs. The board is responsible for creating a culture that places a high priority on compliance and holds management accountable.

The OCC expects the board to be responsible for confirming that a system of internal controls is in place.[101] The board should periodically receive information about the effectiveness of the bank's internal controls and information systems. The board should demonstrate that it has an adequate understanding of the bank's IT infrastructure, inherent risks, and existing controls.

Management's Responsibilities

The OCC expects senior management to be responsible for developing and maintaining the risk governance framework and system of internal controls, which enables management to effectively identify, measure, monitor, control, and report risk exposures consistent with the board-established risk appetite. Senior management should report to the board on the bank's overall risk profile, including aggregate and emerging risks. Senior management should provide the board timely, accurate, and reliable information about current and potential risk exposures and their potential impact on earnings, capital, and strategic objectives, particularly under adverse or stress scenarios. Risk reporting should readily identify significant and emerging risks and issues as well as determine areas that need improvement.

Capable management is essential to an effective risk management system. Senior management should be responsible for the implementation, integrity, and maintenance of the risk management system. Senior management should

- keep directors adequately informed about the level and direction of risk.
- implement the bank's or holding company's strategy.
- develop policies that define the bank's risk appetite that are compatible with the strategic goals.
- ensure the strategic direction and risk appetite are effectively communicated and adhered to throughout the bank.
- oversee the development and maintenance of timely, accurate, consistent, complete, and relevant MIS.

The CEO and senior management play a critical role in communicating to the board and managing the bank. Effective communication is important for corporate and risk governance.

[101] Refer to 12 CFR 30, appendix A, II.A. Internal control systems include internal controls and information systems.

The board delegates authority to senior management for directing and overseeing day-to-day management of the bank. Senior management should be responsible for developing and implementing policies, procedures, and processes that translate the board's goals, strategic objectives, and risk appetite and limits into prudent standards for the safe and sound operation of the bank.

Management carries out the bank's day-to-day activities and financial performance. Management should optimize the bank's earnings by investing in good quality assets. Management should measure performance against strategic and operational objectives and ensure that risk exposures remain within risk limits. Management should ensure that capital and liquidity levels (1) are commensurate with the bank's risk profile; (2) support short- and long-term growth plans; and (3) can withstand economic downturns.

Specifically, the CEO and his or her senior management team should be responsible for

- directing and overseeing day-to-day management of the bank.
- implementing a strong risk culture and ethical standards and providing incentives to reward appropriate behavior.
- complying with laws, regulations, and internal bank policies, including policies governing ethics and insider activities.
- developing and implementing an effective CMS.
- executing the bank's strategic plan, and ensuring the adequacy of capital and resources in carrying out the plan.
- developing and administering a risk governance framework that enables management to effectively identify, measure, monitor, and control risk.
- establishing and maintaining an effective system of internal controls.
- maintaining processes, including stress testing when appropriate, to ensure capital and liquidity levels are commensurate with the bank's risks in normal and stressed conditions.
- developing accurate and reliable management information and reporting systems to keep the board apprised of the bank's strategic direction, risk profile, risk appetite, business operations, financial performance, and reputation.
- appropriately allocating staff resources and effectively overseeing personnel.
- establishing talent management and compensation and employee benefit arrangements.
- implementing a corporate governance structure that provides for effective policies and control systems over relationships with related organizations and transactions with insiders.

Management committees may be used to facilitate oversight of day-to-day banking activities. Management should determine which committees are appropriate for its bank and how formal the committees' structure should be. Typical management committee areas include asset liability, credit, compliance, and IT steering.

Examination Procedures

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention beyond the core assessment contained in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook*. Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment.

Scope

These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the corporate and risk governance examination. This determination should consider work performed by internal and external auditors and other independent risk control functions and by other examiners on related areas. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objective. Seldom will every objective or step of the expanded procedures be necessary.

Objective: To determine the scope of the examination of corporate and risk governance and identify examination objectives and activities necessary to meet the needs of the supervisory strategy for the bank.

1. Review the following sources of information and reports. Note any previously identified problems related to corporate and risk governance that require follow-up:

   - Supervisory strategy.
   - Examiner-in-charge's (EIC) scope memorandum.
   - The OCC's supervisory information systems.
   - Previous reports of examination and work papers.
   - Internal and external audit reports and work papers.
   - Bank management's responses to previous reports of examination and audit reports.
   - Customer complaints and litigation. Examiners should review customer complaint data from the OCC's Customer Assistance Group, the bank, and the Consumer Financial Protection Bureau (when applicable). When possible, examiners should review and leverage complaint analysis already performed during the supervisory cycle to avoid duplication of effort.
   - Financial reports (e.g., the Uniform Bank Performance Report) and applicable OCC analytical tools. Identify changes since the prior review.

2. Obtain and review policies, procedures, and reports bank management uses to supervise corporate and risk governance. Consider

   - bylaws of the bank.
   - the national bank's articles or the FSA's charter.

- a list of directors.
- board meeting packages.
- board-level financial performance and key risk reports.
- board and board-level committee reports and meeting minutes.
- board-level committees' written charters.
- director orientation and education material.
- board self-assessments.
- the strategic plan and reports used to monitor the plan.
- operational plans.
- a list of new, modified, or expanded products and services and documentation of the approval process.
- third-party relationship risk management, including policies and processes.
- the capital plan.
- the risk governance framework, including the risk management system in place.
- executive and frontline unit reports.
- internal risk assessments.
- policies and procedures.
- quality control reviews.
- quality assurance reviews.
- the employee compensation and benefits program information.
- the compliance management program, including the BSA program. (Refer to the *FFIEC BSA/AML Examination Manual* for procedures to evaluate the BSA/AML compliance program.)
- the current CRA public evaluation.
- a schedule of the insurance policies.

3. In discussions with bank management, determine if there have been any significant changes (for example, new executive officers; new directors; changes in corporate structure; changes in the corporate and risk governance framework; strategic and capital plans; changes to charters, policies, procedures, or reports regarding corporate and risk governance; compensation and benefits; and insurance) since the previous examination of corporate and risk governance.

4. Based on an analysis of information obtained in the previous steps, as well as input from the EIC, determine the scope and objectives of the corporate and risk governance examination.

5. Select from the following examination procedures the necessary steps to meet examination objectives and the supervisory strategy.

Board of Directors and Management

Conclusion: The board of directors is (effective or ineffective) in its fiduciary duties and establishing a corporate and risk governance framework to facilitate oversight of bank activities. Management is (effective or ineffective) in directing and overseeing the day-to-day activities of the bank.

Board Composition and Qualifications

Objective: To determine if the board is composed of individuals with a balance of skills, expertise, and diversity who can exercise independent judgment; provide a credible challenge to management's recommendations and decisions; and comply with board-related laws and regulations.

Statutory and Regulatory Requirements

Objective: To assess compliance with laws, regulations, and prudent banking practices relating to board composition and qualifications.[102]

1. Obtain a list of directors that includes the following information for each director:

   - Home address, when appropriate (if the director was appointed or elected since the previous examination, indicate the number of years residing at his or her present address).
   - Years as a director of the bank.
   - Occupation.
   - Citizenship (for national banks).
   - Common stock ownership (beneficial, direct, or indirect) for national banks or membership for mutual FSAs.
   - Bonus, fees, and any other compensation.
   - Attendance record at board meetings.

2. Determine if the number of directors aligns with the bank's bylaws.

3. Determine whether the bank complies with the following laws and regulations regarding director qualifications:

   - Do all directors of national banks possess sufficient stock to qualify as directors? (12 USC 72 and 12 CFR 7.2005)

[102] For a list of the requirements regarding size, composition, and other aspects, refer to this booklet's appendix A, "Board of Directors Statutory and Regulatory Requirements."

- For a stock FSA, do the bylaws require a director to be a stockholder? If so, do all directors meet this requirement? (12 CFR 5.22(l))
- For a mutual FSA, are all directors members of the association? (12 CFR 5.21(j)(2))
- Are all national bank directors citizens of the United States? If not, has the Comptroller waived the citizenship requirement? (12 USC 72) (The majority of directors must be U.S. citizens.)
- Do the majority of national bank directors reside in the state, territory, or district in which the bank is located, or within 100 miles of the bank's main office? If not, has the Comptroller waived the residency requirements? (12 USC 72)
- Did the majority of the national bank directors reside in the state, territory, or district in which the bank is located, or within 100 miles of the bank's main office, for one year before their election? If not, has the Comptroller waived the residency requirements? (12 USC 72)
- Did all national bank directors take an oath of office? (12 USC 73 and 12 CFR 7.2008)
- Did the national bank forward a copy of the oath of office to the OCC? (12 USC 73 and 12 CFR 7.2008)
- Has it been determined that no director is an indenture trustee? (15 USC 77jjj)

4. For FSAs, determine if the bank complies with 12 CFR 163.33.

   - Are the majority of the directors not salaried officers or employees of the FSA or any subsidiary thereof?
   - Are no more than two of the directors members of the same immediate family?
   - Is there no more than one director who is an attorney with a particular law firm?

5. For FSAs, determine if there was a director removed for cause. Cause is defined in 12 CFR 5.21(j)(2)(x)(B) to include personal dishonesty; incompetence; willful misconduct; breach of fiduciary duty involving personal profit; intentional failure to perform stated duties; willful violation of any law, rule, or regulation (other than traffic violations or similar offenses); or final cease-and-desist order.

   - Was a meeting of shareholders called expressly for the purpose of removal for cause, as required? If so, other requirements apply for votes for removal. (12 CFR 5.22(l)(6) for stock FSAs)

6. For FSAs, determine, through examination findings and discussions with examiners, whether the person who has a fiduciary duty to the FSA advanced his or her personal or business interests at the expense of the bank. (12 CFR 163.200)

7. For FSAs, determine, through examination findings and discussions with examiners, if the director, officers, or persons having power to direct management or policies, or persons otherwise owing a fiduciary obligation to the FSA, have taken advantage of corporate opportunities that belonged to the bank. (12 CFR 163.201)

8. Determine if the bank complies with the following laws and regulations regarding board structure:

    - Is the number of directors consistent with the bylaws and no fewer than five and no more than 25 for national banks? (12 USC 71a) If the national bank has more than 25 directors, has the Comptroller waived the 25-director maximum?
    - For FSAs, do the bylaws state a specific number of directors and not a range? (12 CFR 5.22(l)(2) for stock FSAs and 12 CFR 5.21(j)(2)(viii) for mutual FSAs)
    - Is the number of directors consistent with the bylaws and no fewer than five and no more than 15 for FSAs? (12 CFR 5.22(l)(2) for stock FSAs and 12 CFR 5.21(j)(2) for mutual FSAs) If not, has the Comptroller waived the requirements?
    - Did the board appoint directors to fill vacancies? (12 USC 74 for national banks, and 12 CFR 5.22(l)(5) for stock FSAs and 12 CFR 5.21(j)(2) for mutual FSAs)
    - Did shareholders or members elect directors at their regular annual meeting? (12 USC 71 for national banks, and 12 CFR 5.22(k)(1) for stock FSAs and 12 CFR 5.21(j)(2)(i) for mutual FSAs)
    - For national banks, if shareholders did not elect directors at their regular annual meeting, were the elections held within 60 days thereof? (12 USC 75)
    - For FSAs, did the FSA hold an annual meeting for the election of directors within 150 days after the end of the association's fiscal year? (12 CFR 5.22(k)(1) for stock FSAs and 12 CFR 5.21(j)(2)(i) for mutual FSAs)
    - Did the mutual FSA establish a nominating committee, if the bylaws permitted, before the submission of nominations? (12 CFR 5.21(j)(2)(xiii))
    - For national banks, is the president a member of the board? (12 USC 76 and 12 CFR 7.2012)
    - For FSAs, do the bylaws require the president to be a director? If so, has the FSA met this requirement?
    - Is the term of office for a director between one and three years for FSAs and not more than three years for national banks? (12 USC 71 and 12 CFR 7.2024(b) for national banks, 12 CFR 5.22(l)(2) for stock FSAs, and 12 CFR 5.21(j)(2)(viii) for mutual FSAs)

9. Determine compliance with the following laws and regulations regarding restrictions on board activities:

    - Has a quorum been present for all board meetings? (12 CFR 7.2009 for national banks, and 12 CFR 5.22(l)(4) for stock FSAs and 12 CFR 5.21(j)(2)(ix) for mutual FSAs)
    - For national banks, do board procedures preclude any director from casting a vote by proxy? (12 CFR 7.2009)
    - For FSAs, were board actions approved by a majority of directors present at any meeting at which there was a quorum? (12 CFR 5.22(l)(4) for stock FSAs and 12 CFR 5.21(j)(2)(ix) for mutual FSAs)
    - If any management officials of the bank or its holding company or holding company affiliates are management officials of an unaffiliated depository bank or depository

holding company, do any of the statutory exceptions (12 USC 3201 et seq.) or regulatory exemptions (12 CFR 26) apply?
- If any directors have been appointed to the board for purposes other than filling vacancies, do the articles provide for such appointments? (12 CFR 7.2007(a))

10. Determine compliance with the following laws and regulations regarding regulatory reporting:

    - If embezzlements, defalcations, misappropriations, mysterious disappearances, or thefts have occurred since the previous examination, did the bank file a Suspicious Activity Report with the appropriate law enforcement agencies and with the U.S. Department of the Treasury? (12 CFR 21.11 for national banks and 12 CFR 163.180(d) for FSAs)
    - Was the Suspicious Activity Report promptly reported to the board as required? (12 CFR 21.11 for national banks and 12 CFR 163.180(d) for FSAs)
    - If the bank has a class of equity securities held by 2,000 or more shareholders and total assets exceeding $10 million, did the bank file reports with the OCC, as required by federal securities law? (12 CFR 11)
    - Was the OCC notified of any change in control or, if in troubled condition, change in senior executive officers since the last examination? (12 USC 1817(j), 12 USC 1831i, 12 CFR 5.50, and 12 CFR 5.51)
    - Does the bank maintain records of directors, executive officers, and principal shareholders and the related interests of these persons and of extensions of credit to these persons? (12 CFR 31 and 12 CFR 215)
    - Has the bank notified executive officers and directors of the requirements to report to the board the outstanding amount of any credit that was extended to the executive officer or directors and was secured by the bank's shares? (12 CFR 31 and 12 CFR 215)
    - For national banks, if the board contains honorary or advisory members, has the bank distinguished between honorary or advisory directors and active directors in published reports? (12 CFR 7.2004)

11. If it was not done in previous examinations, review and brief the bylaws and articles of association of the bank, including any specific provisions related to the requirements of directors, and if a brief exists from previous examinations, update it as appropriate.

12. Read and brief the minutes of shareholders or members' meetings since the last examination. The brief should include a list of directors elected at the annual meeting, the number of shares present and voted (for national banks and stock FSAs), individuals acting as proxies, and specific action approved by shareholders or members.

13. For stock FSAs, assess whether the minutes reflect a director's dissent or abstention to the board's action to avoid the appearance of approval. (12 CFR 5.22(l)(10))

14. Determine whether all requirements were met (e.g., shareholder approval) for any of the following actions that the board took since the last examination:

- Any change in location of the main or home office. (12 CFR 5.40)
- Any issuance of preferred stock. (12 CFR 5.46 for national banks and 12 CFR 5.22(g)(4)(B) for stock FSAs)
- Any increase in capital stock, either through sale or through a stock dividend. (12 CFR 5.46 for national banks and 12 CFR 5.22(g)(4) for stock FSAs)
- Any reduction in capital stock. (12 CFR 5.46(h) for national banks and 12 CFR 5.22(g)(4) for stock FSAs)
- Any stock split. (12 CFR 5.46 for national banks and 12 CFR 5.22(g) for stock FSAs)
- Any bank pension plan established. (29 USC 1001 et seq.)
- Any bank involvement in a conversion, merger, or consolidation. (12 CFR 5.24 and 12 CFR 5.33 for national banks, and 12 CFR 5.23 and 12 CFR 5.33 for FSAs)
- Matters subject to vote at shareholder meetings. Verify that
  - for national banks, shares held by the bank as sole trustee or in its nominee name are not voted for directors unless applicable requirements are satisfied. (12 USC 61)
  - for stock FSAs, treasury shares held by the FSA and shares held by another corporation, if a majority of the shares entitled to vote for the election of directors of such other corporation are held by the FSA, shall not vote for directors. (12 CFR 5.22(k)(6)(ii) "")
  - for national banks, no officer, clerk, teller, or bookkeeper acted as a proxy. (12 USC 61 and 12 CFR 7.2002)

15. Review any stock option or stock purchase plan adopted since the preceding examination, and review such action for compliance with the articles of association and the various conditions of the articles of association.

16. Determine if any candidate was nominated director, other than the slate nominated by bank management, and whether shareholders submitted new business, and review for compliance with the requirements in 12 CFR 5.22(k)(7) for stock FSAs and 12 CFR 5.21(j)(2)(xiii) and 12 CFR 5.21(j)(2)(xiv) for mutual FSAs.

Core Competencies of the Board

Objective: To determine if the board is well-diversified and composed of individuals with a mix of knowledge and expertise in line with the bank's size, business strategy, risk profile, and complexity.

1. Are background checks performed on board candidates?

2. In the director's selection process, are the candidate's ethical standards and integrity in his or her personal and professional dealings considered?

3. Has the board established a board meeting attendance policy?

4. Is attendance monitored to determine the director's level of involvement and participation?

5. Is there evidence of a credible challenge of management's decisions and recommendations recorded in the board meeting minutes?

6. For national banks, verify that directors have not voted by proxy.

Board Independence

Objective: To determine if the board exercises independent judgment.

1. In assessing whether the board exercises independent judgment, consider whether

   - there is a mix of independent and management directors.
   - there is a dominant management or director(s).
   - the board has adopted standards on conflicts of interest and independence.
   - the board convenes executive sessions without management's influence.

2. Determine if the CEO also serves as the board chair. If so, does the bank also have a lead director who is independent of management to provide a balance of power?

3. For covered banks, verify that at least two members of the board are independent directors. (12 CFR 30, appendix D)

   - Independence means the individual
     – is not an officer or employee of the bank or parent company and has not been an officer or employee of the bank or its parent company in the past three years.
     – is not an immediate family member of a person who has been an executive officer of the bank or its parent company in the past three years.
     – qualifies as an independent director under the listing standards of a national securities exchange.

Outside Advisors and Advisory Board

Objective: To determine if the board uses advisors to leverage expertise independent of bank management, when appropriate.

1. Determine if the board has a process in place to solicit outside advisors, when appropriate.

2. Determine if the board has used an outside advisor since the last examination. If so, obtain a copy of the engagement letter and the information and expert advice provided to the board or designated committee.

3. Assess if the fees charged are reasonable and in line with the services rendered.

4. If the bank uses advisory directors, does the board ensure that they do not have voting privileges?

Board Practices

Objective: To determine if the board adopted practices that permit effective oversight based on the size, strategy, risk profile, and complexity of the bank.

Board Information

Objective: To determine if the information provided to the board is adequate to make informed decisions and allow directors to provide a credible challenge to management assertions.

1. Determine whether management provides information to the board that is accurate, complete, and timely and is presented in a meaningful format to allow for effective oversight.

2. Determine whether the information is periodically reviewed by internal audit for integrity.

3. Does the information include key performance measurements and key risk indicators to monitor adherence to the bank's strategy and risk appetite?

4. Does the board periodically reevaluate the information it receives to determine if it has sufficient information to make informed decisions?

Meetings and Minutes

Objective: To determine if board meetings and minutes reflect the material issues of the bank and comply with board meeting-related laws and regulations.

1. For national banks, mutual FSAs, and stock FSAs, determine the date of the annual shareholders' or members' meeting, and verify that the date was in compliance with the bylaws. (12 USC 71 for national banks,12 CFR 5.21(j)(2)(i) for mutual FSAs, and 12 CFR 5.22(k)(2) for stock FSAs)

2. Review the bank's practice of notifying shareholders or members of special or regular meetings.

    - For national banks, at least 10 days' notice is required, and the notice must include the time, place, and purpose of the meeting. Longer periods may be required by the articles of association, the bylaws, or other laws and regulations applicable to a national bank. (12 USC 75 and 12 CFR 7.2001)
    - For stock FSAs, notice delivered not fewer than 20 days nor more than 50 days is required. The notice must state the place, day, hour, and purpose of the meeting. (12 CFR 5.22(k)(2))
    - Mutual FSAs must publish notice for two successive weeks immediately before the week in which the meeting will convene, in a newspaper of general circulation in the city or county in which the principal place of business of the association is located.

Alternatively, the FSA may mail notice at least 15 days and not more than 45 days before the date of the meeting to each of its members. In addition to following one of these alternatives, the mutual FSA must post a notice of the meeting in a conspicuous place in each of its offices during the 14 days immediately preceding the date of the meeting. (12 CFR 5.21(j)(2)(iii))

3. For mutual FSAs, determine if directors receive notice of a board meeting at least 24 hours in advance unless the directors waived notice. (12 CFR 5.21(j)(2)(ix))

4. For stock FSAs, determine if directors receive notice of special board or board committee meetings at least 24 hours in advance unless the directors waived notice. (12 CFR 5.22(l)(8))

5. Determine if the frequency of board and board committee meetings is sufficient to manage the affairs of the bank.

6. Determine if the board receives board packets in advance to allow directors to prepare for meetings.

7. Determine whether the information packets cover key risks of the bank.

8. Read and brief the minutes of all meetings of the board since the last examination. Note the following:

   - Any actions taken in contravention of the bylaws.
   - Actions taken by the board that are not part of a normal monthly meeting.
   - Resolutions or discussions about entrance into a new geographic area, customer service, asset or liability category, or other new undertaking. This also should include a discussion of updates to the strategic plan and how any new activities fit in with the plan.
   - Creation of any special committee and its mission.
   - Ratification by the full board of actions taken by standing committees.
   - Any transactions with directors or their interests, or abstention of any interested director. If the minutes do not mention any director-related transactions that are uncovered during the examination, determine why the identified transaction was not discussed during a board meeting. Also determine how the director-related transaction was approved and whether the interested party refrained from voting.
   - Director attendance to determine the levels of interest and dedication, and how the directors fulfill fiduciary responsibilities.
   - Participation of individual directors to determine if any one, or a certain group of directors, dominates the board discussions.
   - Re-booked charged-off loans approved by the board and the rationale for re-booking. (**Note:** The re-booking of charged-off loans is inconsistent with both generally accepted accounting principles and the call report. It is an unacceptable practice.) Distribute list to examiner assigned Loan Portfolio Management and inform the EIC.
   - Reviews of correspondence between the OCC and the bank.

- Reports of examinations and audits reviewed and actions taken or plans to effect correction of deficiencies.
- Whether directors of an FSA reviewed the results of operations with respect to interest rate risk exposure at least quarterly and made appropriate adjustments as necessary. (12 CFR 163.176)
- Whether directors reviewed and approved written policies, at least annually, that establish appropriate limits and standards for extensions of credit that are secured by real estate. (12 CFR 34, subpart D, and subpart D, appendix A, for national banks and 12 CFR 160.101 and appendix for FSAs)
- Whether directors designate a security officer to report at least annually on the implementation, administration, and effectiveness of the security program. (12 CFR 21, subpart A, for national banks and 12 CFR 168 for FSAs)

9. Determine if documentation of board meeting minutes is sufficient to determine

- the board's review and discussion of material action items on the agenda.
- actions taken.
- abstention of votes.
- follow-up items to be addressed at a later meeting.
- attendance of each director and other attendees.
- previous board meeting minutes' approval.
- board-approved policies.

Policy Review and Approval

Objective: To determine if the board has a process to review and approve policies.

1. Are policies that are statutorily required to be reviewed and approved by the board done so in accordance with the respective regulations?[103]

2. Does the board require periodic reviews of policies to confirm that they are consistent with the bank's strategic objectives, risk appetite, and regulatory requirements?

3. Has the board established a method to measure and monitor compliance with board-approved policies?

4. Assess the board's process to address instances when the bank is approaching or has breached a policy limit.

[103] For a list of the statutorily required policies and programs requiring board approval, refer to this booklet's appendix B.

Director Orientation and Education

Objective: To determine if the board has an education program that keeps its members apprised of major bank operations and industry trends.

1. Determine if the bank has an orientation and education program to provide training on the bank's business, risks, and operations, and to help directors stay apprised of industry trends and regulatory developments.

2. Determine if there is a process to periodically assess the skills and competencies of members and address any identified gaps.

3. For covered banks, has the board established and complied with a formal, continuous training program for all directors? (12 CFR 30, appendix D)

4. When appropriate, does the board engage outside advisors to gain technical expertise? If so, has it ensured that there is no conflict of interest that would prohibit the consultant from providing objective, independent advice?

Board Oversight

Objective: To determine if the board is fulfilling its responsibility to effectively supervise the affairs of the bank.

Corporate Culture

Objective: To determine if the board and management, in their respective roles, have established a sound corporate and risk culture.

1. What measures has the board taken to set the tone at the top?

2. Determine through discussions with management and employees if they are aware of the bank's risk culture, the parameters that they must operate in, and the steps that they should take if there is any breach of the bank's risk appetite and limits.

3. Has the board adopted a code of ethics and respective policies that set expected standards of behavior for all employees and directors?

4. How is adherence to the code of ethics monitored and managed?

5. Are consequences clearly communicated and consistently enforced for behaviors that contravene the bank's code of ethics?

6. Determine whether suspected fraud; illegal or unethical activities; and material risk issues are thoroughly and independently investigated by management and escalated to the board promptly.

7. Is there an ethics officer, bank counsel, or other individual from whom employees can seek advice for ethics questions?

8. Does the bank's internal auditor periodically assess the effectiveness of the bank's code of ethics program?

Board Committees

Objective: To determine if the board committees enable the board to carry out its oversight duties and responsibilities.

1. Has the board established a committee structure based on the bank's needs? Does each board committee have a charter?

2. Determine the level of involvement of directors based on a review of the committee meeting minutes.

3. Is director participation on various committees aligned with the directors' experience and expertise?

4. Are committee members periodically rotated to promote objectivity and different perspectives?

5. Read and brief the minutes of the board's annual organization meeting and list standing committees and their members. Some examples of committees a bank may have, depending on its size, scope of operations, risk profile, and board composition, include

   - executive committee.
   - audit committee (required by 12 CFR 363 for banks with assets over $500 million).
   - credit committee.
   - asset-liability management committee.
   - risk committee.
   - fiduciary committee.
   - fiduciary audit committee (required by 12 CFR 9 (national banks) and 12 CFR 150 (FSAs) if trust powers are active).
   - compensation committee.
   - corporate governance/nominating committee.

6. Read and brief the minutes of the standing committees as well as ad hoc committees in their assigned areas, specifically noting whether each committee's mission, authority, and responsibilities are clear and followed.

7. Note major areas of operation that are not monitored by specific committees and determine if this information is communicated to the board.

Board Self-Assessments

Objective: To determine if the board periodically evaluates its performance.

1. Determine if the board conducts self-assessments. If so, has the board satisfactorily addressed any identified gaps or weaknesses to strengthen its effectiveness and oversight?

2. Determine whether the content of the assessment is linked to the board's charter and activities (i.e., roles and responsibilities)?

3. If the board does not perform a self-assessment, what other means does it use to evaluate its performance?

Risk Governance Framework

Objective: To determine if the board and management, in their respective roles, established a risk governance framework to manage the enterprise-wide risks.

1. Has management developed a risk governance framework commensurate with the sophistication of the bank's operations and business strategies? Has it been reviewed and approved by the board?

2. Does the risk governance framework cover all applicable risks of the bank?

3. Does the board require periodic independent assessments on the effectiveness of the risk governance framework or the components thereof?

4. For covered banks,

   - has IRM designed a written risk governance framework?
   - has the board or a board-level committee reviewed and approved the framework?
   - does IRM review and update the framework at least annually?
   - if the bank has adopted the parent company's risk governance framework, does it meet the standards established in 12 CFR 30, appendix D?

Risk Culture

Objective: To determine if the board and senior management have conveyed the bank's risk culture throughout the bank.

1. Determine how risk awareness is communicated throughout the bank.

2. Are the employees aware of consequences for excessive risk taking?

3. Are material risks and risk-taking activities that exceed the bank's risk appetite escalated and addressed by management or the board in a timely manner?

Risk Appetite

Objective: To determine if the board has established a risk appetite that aligns with the bank's strategic objectives, capital plans, and liquidity requirements.

1. Has the board established a risk appetite that articulates the aggregate level of risk and types of risk the board and management are willing to assume? Has it been formalized as a written risk appetite statement, when appropriate? Is it reviewed and updated periodically?

2. Has the risk appetite been communicated throughout the bank?

3. Have risk parameters and limits been established for specific business lines and for aggregate risks (including concentrations)?

4. If the bank approached or breached a risk limit, was the issue reported to the board or a board-level committee and senior management? Was a plan of action developed to address the risk-limit breach?

5. Has management established an escalation process that escalates weaknesses or problems to the board and senior management, when appropriate?

6. For covered banks,

   - does the bank have a written statement that articulates the bank's risk appetite?
   - does the board or risk committee review and approve the risk appetite statement at least annually?
   - does the statement include both quantitative limits and qualitative components?
   - is the risk appetite statement integrated and consistent with the overall strategy?
   - has IRM established enterprise policies that include concentration risk limits?

Risk Assessment

Objective: To determine if the bank has an effective risk assessment process to continuously identify current and emerging risks.

1. Does the bank prepare risk assessments on material activities at least annually?

2. Are risk assessments integrated into the bank's strategic planning process and risk management activities?

3. Do the risk assessments identify current risks and controls as well as new and emerging risks? Are the risk assessments candid and self-critical?

4. Are the assessments used to determine if actions need to be taken to strengthen risk management or reduce risk?

Risk Management System

Objective: To determine if the bank has adopted a risk management system commensurate with its size, complexity, and risk profile.

1. Does the structure of the risk management system allow for the bank's risks to be appropriately identified, measured, monitored, controlled, and reported to the board and senior management?

2. When appropriate, is there an IRM function that oversees the risk activities of the bank?

3. If there is not an IRM function, does the bank have sufficient management oversight of the bank's risk-taking activities, aggregate risks, and concentrations to confirm compliance with the bank's risk appetite?

4. If the bank does not have a CRE, has the board appointed a qualified individual or committee to oversee the bank's ERM program?

5. If the bank has adopted the three lines of defense,

    - is the first line of defense (frontline units or business units) accountable for assessing and managing the risk that the frontline units create?
    - has the first line of defense established internal controls that are consistent with the established risk appetite and risk limits?
    - has the first line of defense established controls for compliance with laws and regulations?
    - is the second line of defense (IRM) led by a CRE who has sufficient stature in the bank?
    - does the IRM function oversee risk-taking activities and assess risk independent of the frontline units?
    - is IRM monitoring compliance with the risk appetite and reporting findings to the board?
    - is IRM involved in management's key risk decisions?
    - is IRM identifying, measuring, monitoring, and controlling aggregate and emerging risk enterprise-wide?
    - is the third line of defense (internal audit) providing assurance on the effectiveness of the bank's risk management system?

6. For covered banks, determine compliance with 12 CFR 30, appendix D.

    - Does the risk governance framework include risk management roles and responsibilities for frontline units, IRM, and internal audit?

- Do the frontline units continuously assess the material risks associated with their activities?
- Does IRM oversee the bank's risk-taking activities, assess risk and issues independent of frontline units, and identify and assess aggregate risks and concentrations across the bank?
- Does internal audit ensure that the bank's risk governance framework complies with the guidelines?
- Does internal audit maintain an inventory of the bank's material processes, product lines, services, and functions and assess the risk associated with each when developing the audit plan?
- Does the board actively oversee the bank's risk-taking activities and hold management accountable for adhering to the risk governance framework?
- Does the board conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards in section III of 12 CFR 30, appendix D?

7. Has the board or audit committee required a periodic independent assessment of the bank's overall risk governance framework and risk management practices? If so, was an opinion provided on the design and effectiveness of the framework?

Audit Program

Consult with the examiner assigned the audit review. For expanded examination procedures, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

Objective: To determine the effectiveness of the board's oversight of the internal and external audit functions.

1. Based on the results of the examination of the bank's internal audit function, assess the adequacy of the function within the risk governance framework. Consider

   - independence of auditors, including reporting lines.
   - qualification of auditors.
   - adequacy and appropriateness of audit program.
   - degree and effectiveness of audit committee oversight.

Strategic Planning

Objective: To determine the effectiveness of the bank's strategic planning process.

1. Does the bank have a board-approved written strategic plan? If not, how are strategic objectives communicated throughout the bank?

2. Is the strategic plan aligned with the bank's risk appetite, capital plan, and liquidity requirements?

3. Does the bank have a strategic planning process that considers

   - an analysis of the bank's strengths, weaknesses, opportunities, and threats including regulatory, economic, competitive, and technological matters?
   - the bank's mission, goals, and measureable objectives?
   - assessment of risk associated with the strategies and whether they are in line with the bank's risk appetite?
   - the resources needed to achieve objectives, including technology requirements and constraints?
   - the contingency plans for significant unanticipated events?
   - the formality of the planning process based on the bank's size, complexity, and risk profile?

4. When the bank has engaged in merger or acquisition activities, has the bank performed a retrospective review of the merger that considered, at a minimum, the effect on

   - financial performance (sales, costs, etc.)?
   - accounting?
   - IT infrastructure (system integration, capacity, etc.)?
   - human resources?

5. Determine whether the long-term (strategic) plan provides the framework for developing short-term (operating) plans.

6. Determine how management verifies compatibility between the short-term and long-term plans by considering the

   - annual financial plan and budget.
   - capital plan.
   - asset-liability plan.
   - marketing plan.
   - fixed-asset plan.

7. Determine whether management weighs the effects of plans on its operations. Consider

   - risk.
   - regulatory requirements.
   - financial condition of the bank.
   - management ability and human resource demands.
   - physical facilities.
   - adequacy of MIS and operating systems to handle growth.
   - current product mix and future product development.
   - technological environment.
   - public perception.

8. Determine if the bank has monitoring and reporting routines to determine the bank's progress in achieving its strategic objectives. Consider

    - frequency and method of evaluation.
    - CEO and board of director involvement.
    - accountability of managers to implement plans and achieve objectives.
    - if there is a system in place to make changes.
    - if there is a system in place to report on progress toward goals.
    - flexibility in the plan to allow for contingencies or changes.

9. For covered banks, does the strategic plan cover, at a minimum, a three-year period and comply with the standards in section II of 12 CFR 30, appendix D?

New Activities

Objective: To determine the adequacy of the bank's risk management system to identify, measure, monitor, report, and control risks when developing and implementing new activities. Refer to OCC Bulletin 2017-43 for more information.

1. Determine the adequacy of the bank's due diligence and approval process for new activities. Due diligence should allow management to fully understand the risks and benefits before implementing new activities. Management should inform the board of all material new activities, including due diligence findings and plans that clearly articulate and appropriately manage risks and returns. The board or a delegated board committee should consider whether new activities are consistent with the bank's strategic goals and risk appetite. Consider whether due diligence includes

    - identifying the customer demand for the proposed new activities. Consider the types of market research the bank uses, such as surveys, focus groups, and outside services.
    - assessing whether the risks associated with the proposed new activities are consistent with the bank's strategic plan, risk profile, and risk appetite.
    - assessing how the new activity affects the bank's current and projected capital position.
    - consulting with relevant functional areas, which include credit, asset management, payments, compliance, accounting, audit, independent risk management, legal, operations, IT, information security, marketing, and the treasury/asset liability committee, to identify risks, concerns, and necessary controls.
    - determining the requirements of applicable laws and regulations and considering the principles set forth in agency guidance.
    - identifying potential conflicts of interest, actual or perceived.
    - assessing potential negative effect on the bank's reputation.
    - appropriately protecting any intellectual property rights.
    - determining the expertise needed to effectively manage the new activities, including the possible need to hire or otherwise acquire additional expertise.

- determining the operational infrastructure requirements to support the new activities, including controls and technology architecture.
- conducting appropriate research and analysis on relevant third-party service providers.
- developing a business and financial plan that includes
  - expected costs.
  - sales revenue targets.
  - an assessment of the bank's competitive position if the bank engages in the new activities.
  - objectives and strategies for how the new activities will be brought to market.
  - consideration of fair access to financial services and fair treatment of customers in all aspects related to the new activities.
  - performance or risk metrics that signal the need to pursue an exit strategy.
  - viable alternatives, including an exit strategy, in case the new activities fail to perform as expected

2. Assess whether management has established appropriate policies, processes, and control systems for new activities. Consider whether

   - policies and procedures outline the processes, roles, and responsibilities for implementation and adherence to an adequate risk management system for new activities.
   - management expands or amends, as appropriate, existing policies and procedures to adequately address the new activities. Do policies and procedures identify key business lines, establish management's responsibility for monitoring the process, and provide for exception reporting?
   - management develops and deploys MIS as necessary to monitor adherence to established objectives and to properly evaluate the new activities, and, if warranted, effectuate a timely response.
   - new activities are incorporated into the bank's independent risk management, CMS, and audit processes to verify adherence to bank policies and procedures and customer safeguards.
   - the bank has adequate third-party risk management policies and procedures in place, when applicable.

3. Assess the effectiveness of change management processes to manage and control the implementation of new or modified operational processes, as well as the addition of new technologies into the bank's existing technology architecture. Consider whether change management processes include

   - reviews by appropriate risk management, line managers, and senior managers in applicable business units (such as lending, finance, treasury, deposits, payments, compliance, audit, legal, technology, and information security) before implementing the new or modified operational process.
   - proper testing of new or modified operational systems, processes, and technology.

- risk parameters and exception reporting that have been approved by appropriate management.
- mechanisms for confirming that delivery to customers occurs as intended.
- an exit strategy that identifies and limits the adverse effect to the bank and its customers in the event of a failed or flawed implementation.
- employee training in the new or modified operational process associated with the new activities.

4. Assess the bank's performance and monitoring systems for new activities. Consider whether such systems

- include limits on the size of risk exposure that management and the board are willing to accept with the addition of new activities.
- identify specific objectives and performance criteria to evaluate whether the new activities are successful, including processes to periodically compare actual results with projections, and quantitative and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- include processes to periodically test the effectiveness of operational controls and safeguards.
- include periodic testing to ensure compliance with applicable laws, regulatory requirements, and the bank's policies and procedures. This should include consideration of potential risks for unfair or deceptive acts or practices.
- trigger changes in the business plan for the activities, based on performance results, including an exit strategy for activities that fail to achieve projections.

Capital Planning

Consult with the examiner assigned to review the capital component area. For examination procedures, refer to the "Capital and Dividends" booklet of the *Comptroller's Handbook*.

Recovery Planning

For examination procedures, refer to the "Recovery Planning" booklet of the *Comptroller's Handbook*. These procedures only apply to covered banks subject to 12 CFR 30, appendix E.

Operational Planning

Objective: To determine the adequacy of the bank's operational plans that translate long-term strategic objectives and goals into measureable targets.

1. Determine what operational plans are in place. Consider

- budgets.
- marketing plans.

- staffing plans.
- contingency plans.

2. Assess the formality of the operational planning process to determine whether it is commensurate with the bank's size, complexity, and risk profile.

3. Confirm that operational plans are board-approved and are periodically reviewed and updated.

4. Determine the adequacy of operational plans. Consider whether plans

   - are consistent with the bank's risk appetite and strategic plan.
   - adequately translate long-term strategic objectives and goals into measurable targets.

Disaster Recovery and Business Continuity Planning

Consult with the examiner assigned to review the IT component area. For examination procedures, refer to the "Business Continuity Planning" booklet of the *FFIEC IT Examination Handbook.*

IT and Information Security

Consult with the examiner assigned the IT component area to assess the bank's IT infrastructure. For examination procedures, refer to the "Information Security" and other booklets of the *FFIEC IT Examination Handbook.*

Management Selection, Retention, and Oversight

Objective: To determine whether the directors have accepted their responsibility for selecting and retaining competent management.

1. Determine if the board has defined specific selection criteria, including experience, expertise, and personal character, for the CEO selection process.

2. Determine how the board assesses senior management's performance. Has the board adopted a performance appraisal process for the CEO and other key executives?

3. Determine whether the board or a committee thereof reviews the CEO's performance at least annually. If so, review the criteria considered for reasonableness. Evaluation criteria may include

   - the bank's record of compliance with laws and regulations.
   - weaknesses contained in audit and examination reports, and their resolution.
   - management's responsiveness to board directives, including compliance with board-approved policies.
   - the timeliness, quality, and accuracy of management's recommendations and reports.

- management's presentations to the board.

4. Determine if the board or a committee thereof reviews the performance of key management members at least annually. Coordinate the assessment of such performance reviews with the EIC and the examiner assigned to the management component rating in CAMELS.

5. Determine if a board-approved management succession policy exists to address the loss of the CEO and other key executives.

6. Discuss planned changes to management positions with the EIC and appropriate bank officials. Determine the rationale for changes.

7. If vacancies exist in senior-level management positions, determine if, when, and how the vacancies will be filled. Also determine the board's criteria to fill those vacancies.

8. Obtain a copy of any management contracts. Brief the pertinent points and determine whether the bank has had appropriate legal review of the contracts and whether any terms would result in unsafe or unsound practices.

9. For FSAs, determine whether the board annually reviews and approves all employment contracts and compensation arrangements for senior officers and directors. (12 CFR 163.39)

10. Determine the reasonableness of compensation of executive officers, how compensation is determined, and who makes decisions concerning executive salaries. (12 CFR 30, appendix A)

11. Note any titled individual who, by action of the board or by the bylaws, is specifically excluded from being an executive officer. (12 CFR 31 and 12 CFR 215.2(e)) Be alert for any policymaking decisions made by any titled officer specifically excluded from being an executive officer.

12. Is succession planning regularly discussed at board or board committee meetings?

13. For covered banks, has the board or board committee reviewed and approved a written talent management program for the CEO, CAE, and CRE; their direct reports; and other potential successors?

Compensation and Benefits Programs

Objective: To determine if compensation and benefits programs are prudent and comply with applicable laws and regulations.

1. Obtain a list of the compensation and benefits of senior management and the board.

2. Determine the reasonableness of the compensation and benefits of senior management and the board given the financial condition and risk profile of the bank.

3. Determine whether appropriate internal controls are in place for employee benefits and are functioning as designed. Complete the internal control questionnaire (ICQ) in this booklet, if necessary to make this determination.

4. Has the board confirmed that compensation practices for directors, executive officers, employees, and principal shareholders are reasonable, are consistent with regulatory guidelines (12 CFR 30, appendix A), and comply with applicable regulations (e.g., 12 CFR 359 and 12 CFR 1026.36 (national banks and FSAs), and 12 CFR 163.39(a) (FSAs))?

5. Does the board oversee and set the compensation of the CEO and other executive-level officers? If so, is the board

   - evaluating employment contracts?
   - periodically assessing the reasonableness of the compensation structure and components, including various benefits and perks related to retirement, termination, and change in control?
   - evaluating executive performance relative to board-established goals and objectives?

6. Determine the degree to which incentive compensation arrangements are used.

7. If incentive compensation arrangements are in place, select a sample and assess the following:

   - Incentives appropriately balance risk and reward.
   - Compensation is compatible with the bank's controls and risk management.
   - Oversight of incentive compensation arrangements is supported by strong corporate governance, including active oversight by the board.

8. Does the bank have risk management practices for benefits administration that safeguard against regulatory fines and lawsuits?

9. Verify that the board oversees the cost and scope of employee benefits and management's role in the administration of benefits.

10. If the benefits administration is outsourced, does management provide oversight to the function to confirm compliance with applicable laws and regulations?

11. If the bank offers a group health plan or retirement plan, assess whether a process is in place to meet the bank's fiduciary responsibilities under the Employee Retirement Income Security Act of 1974 (29 USC 1001 et seq.).

12. Determine if internal audit periodically reviews the bank's compensation and benefits programs.

Financial Performance

Objective: To determine if the board has accepted its responsibility to oversee business performance.

1. Review the board-level financial performance and key risk reports to determine the adequacy of information to assist in decision making and for oversight and monitoring purposes.

2. Determine if the board reports

   - are appropriate for the bank's size, complexity, and risk.
   - enable the board to understand key drivers of financial performance.
   - assess the adequacy of capital, liquidity, and earnings, and monitor trends.
   - compare financial performance with strategic objectives.
   - monitor risk exposure compared with the bank's risk appetite.
   - disclose model risks and reliance.
   - highlight risks related to technologies and market conditions.
   - inform the board of potential litigation costs.

3. Determine if the board compares the bank's performance with that of its peers and, if so, how that comparison is used.

Corporate Structure and Affiliate Relationships

Objective: To determine if the board maintains appropriate affiliate and holding company relationships.

1. Assess whether the bank maintains sufficient independence in its relationships with its parent company and other related organizations so that the bank's interests are adequately protected and not subordinate to those of the related organizations. For examination procedures for national banks, refer to the "Related Organizations" booklet of the *Comptroller's Handbook*. For FSAs, refer to section 730, "Related Organizations," of the *OTS Examination Handbook.*

Community Reinvestment Act

Objective: To determine if the board understands management's involvement in the community and assessed the bank's efforts toward meeting the credit needs of the bank's communities.

1. Discuss the bank's CRA efforts with the examiner conducting the CRA evaluation and the EIC. If a CRA evaluation is not being done concurrently, discuss the bank's efforts with the President or CEO and review the following information:

   - Current CRA public file.
   - Most recent CRA performance evaluation.
   - Information contained in the OCC database (i.e., community contacts and community group protests).

2. Have the board and management, in their respective roles, assessed how the bank is helping to meet the credit needs of its community as part of the strategic planning process?

Policies

Objective: To determine if management has developed adequate policies for all significant areas of the bank.

1. Determine the adequacy of the policymaking process, taking into account

   - regulatory requirements.
   - risks and risk appetite.
   - strategic, operating, and capital plans and liquidity requirements.
   - the bank's condition.
   - differences between planned goals and current conditions.
   - the process to review, update, and revise policies.

2. Obtain or update a list of all board-approved policies and verify that they cover the significant activities and risks of the bank.

3. Determine how management verifies that adopted policies are followed and that exceptions are documented.

4. Determine if policies are appropriate and consistent with the bank's strategic objectives and risk appetite. (Some testing may be necessary to complete this procedure.) This should be done in conjunction with the examiners reviewing each area of the bank.

5. Verify that policies assign accountability and are communicated to appropriate personnel.

6. Review findings from examination work papers or in discussion with other examiners to determine the overall adequacy of the bank's policymaking process.

Processes

Objective: To determine the adequacy of bank operating procedures, programs, and practices.

1. Confer with the EIC and other examiners to determine the adequacy of the bank's procedures, programs, and practices regarding their areas of review. Consider whether

   - procedures are in place for key policies.
   - procedures are communicated to appropriate personnel and made readily available for reference.
   - procedures are periodically reviewed and updated to reflect current practices.
   - appropriate programs are in place to manage key banking activities and risks.
   - bank practices are in line with
     – strategic goals and objectives.
     – risk appetite.
     – laws and regulations.
     – policies.

Personnel

Objective: To determine the skills and qualifications of personnel to fulfill duties and determine if management provides adequate oversight of personnel activities.

1. Determine if the bank has written job descriptions and responsibilities that are clear and reflect assigned duties. Consider the

   - appropriateness of the required knowledge and skills.
   - basis for performance appraisals.
   - method used to develop or oversee the job description process.
   - relationship to compensation program.

2. Assess how management determines that the bank has adequate staff at all levels. Consider

   - recruitment methods.
   - performance standards.
   - training programs.
   - management succession plans.
   - compensation programs.
   - employee benefits.

3. Determine how management assesses employees' performance.

4. Determine how management verifies that salaries and benefits are equitable and competitive.

5. Determine how management promotes effective communication, including the following venues:

- Staff meetings.
- Employee interviews.
- Employee handbooks, bulletins, etc.
- Memorandums, e-mails, and other communications to employees.

Control Systems

Objective: To determine if management has established effective control functions to fulfill its responsibilities and comply with laws and regulations.

1. Determine the control functions that management uses to measure performance, make decisions about risk, and assess the effectiveness of processes, including

   - quality assurance and quality control.
   - audit.
   - risk reviews (including loan review).
   - compliance management.

2. In consultation with the examiner assigned to the audit review, determine if internal and external audit evaluate whether

   - the board and management, in their respective roles, review insider transactions for compliance with laws, regulations, and policies, as well as look for suspicious activity.
   - management takes timely corrective action to address deficiencies noted by the regulatory examination, audit, compliance, or internal loan review functions.

3. Determine the extent to which management is involved in control functions. Consider

   - adequacy, timeliness, and distribution of various reports.
   - periodic review to determine adherence to policies and procedures.

4. Determine the process used by management to confirm that internal controls function properly. Consider

   - sources and accuracy of information.
   - review of internal controls when changes in operations occur.
   - stakeholders involved in the development of new products or changes in operations (audit, IRM, legal, and compliance).
   - training of personnel regarding the bank's policies and procedures.
   - efforts made by directors and managers to correct deficiencies.

5. Determine what quality control activities, if any, the bank performs and assess the effectiveness of the reviews. Consider

- industry standards.
- risk exposures of activities.
- independence of personnel performing review.
- timing of the review.
- results of quality control reports and how they are used to improve risk management.

6. Determine what quality assurance activities, if any, the bank performs and assess the effectiveness of the reviews. Consider

   - industry standards.
   - risk exposures of activities.
   - independence of personnel performing review.
   - timing of the review.
   - results of quality assurance reports and how they are used to improve risk management.

Management Information Systems

Objective: To determine if MIS policies or practices, processes, objectives, and internal controls are adequate.

Note: IT examiner support should be considered to enhance the depth of coverage for the MIS review if there are known MIS issues or deficiencies that represent an undue level of risk or if MIS activities are particularly complex or sophisticated.

1. Evaluate if MIS applications provide the board and management with timely, accurate, consistent, complete, and relevant information.

2. In consultation with the examiners reviewing their assigned areas, determine management's knowledge of information systems and the use of data for decision making.

3. Assess the types and level of risk associated with MIS and the quality of controls over those risks.

4. Determine whether appropriate internal controls are in place for MIS and functioning as designed. Complete the ICQ in this booklet, if necessary, to make this determination.

5. Determine if MIS applications and enhancements to existing systems adequately support corporate and strategic goals.

6. Determine if MIS is being developed in compliance with an approved MIS policy.

7. Determine if management is committed to providing the resources needed to develop the required MIS.

8. For covered banks, determine if the bank has policies, procedures, and processes in place for risk data aggregation and reporting capabilities.

9. If substantive safety and soundness concerns remain unresolved regarding the bank's MIS that may have a material adverse effect on the bank, further expand the scope of the examination by completing verification procedures.

Compliance Management

Consult with the examiners assigned to the consumer compliance and BSA/AML reviews when assessing the effectiveness of the bank's compliance management program. For expanded examination procedures regarding the bank's program for compliance with consumer protection-related laws and regulations, refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook.*

Objective: To determine the effectiveness of the bank's CMS.

1. Confirm that the CMS consists of a compliance program (policies and procedures) as well as a compliance audit function. This includes a BSA compliance program.

   Note: Refer to the *FFIEC BSA/AML Examination Manual* for procedures to evaluate the BSA/AML compliance program.

2. Determine if the board or management has appointed a compliance officer or equivalent who has the authority and stature to effectively manage the compliance function.

3. Have the compliance officer's duties and responsibilities been established and clearly communicated? Responsibilities may include

   - developing a process to identify and stay apprised of all applicable laws and regulations.
   - overseeing and maintaining the inventory of all laws and regulations applicable to the bank and its related organizations.
   - implementing appropriate change management to identify systems, processes, and procedures that are affected by laws and regulation changes.
   - overseeing the establishment of compliance monitoring and testing programs and confirming their adequacy.
   - developing and overseeing metrics for continuous compliance monitoring.
   - overseeing training on all relevant compliance issues.

4. Does the bank's CMS extend beyond consumer protection laws and regulations to include all applicable laws and regulations, prudent ethical standards, and contractual obligations?

5. Is there evidence that the board places a high priority on compliance with laws and regulations? If so, is it communicated throughout the bank?

6. Does the board confirm timely correction and hold management accountable for noncompliance with laws and regulations?

BSA/AML Program

Consult with the examiner assigned the BSA/AML review. Refer to the *FFIEC BSA/AML Examination Manual* for procedures to evaluate the BSA/AML compliance program.

Third-Party Risk Management

Refer to OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures," for procedures to evaluate third-party risk management.

Insurance

Objective: To determine the effectiveness of the bank's risk transference indemnification and insurance.

1. Determine whether the bank has a designated risk manager who is responsible for loss control. If not, determine who handles the risk management and insurance function.

2. Determine whether appropriate internal controls are in place and function as designed for indemnification and insurance. Complete the ICQ in this booklet, if necessary, to make this determination.

3. Determine whether the board has established appropriate maximum guidelines for risk retention.

4. Obtain the bank's schedule of insurance policies in place. If the bank does not maintain a schedule, ask management to create a schedule of existing insurance coverage.

5. Using the insurance schedule prepared by the bank, determine whether coverage conforms to the guidelines for maximum loss exposure established by the board. The summary should include

   - coverage provided, detailing major exclusions.
   - underwriter.
   - deductible amount.
   - upper limit.
   - term of the policy.
   - date premiums are due.
   - premium amount.

6. Determine whether insurance coverage provides adequate protection for the bank.

Conclusions

Conclusion: Corporate and risk governance practices are (strong, satisfactory, insufficient, or weak).

Objective: To determine, document, and communicate overall findings and conclusions regarding the examination of corporate and risk governance.

1. Determine preliminary examination findings and conclusions and discuss them with the EIC.

   - Quantity of associated risks (as noted in the "Introduction" section of this booklet)
   - Quality of risk management
   - Aggregate level and direction of associated risks
   - Overall risk in corporate and risk governance
   - Violations and other concerns

Summary of Risks Associated With Corporate and Risk Governance				
Risk category	**Quantity of risk**	**Quality of risk management**	**Aggregate level of risk**	**Direction of risk**
	(Low, moderate, high)	(Weak, insufficient, satisfactory, strong)	(Low, moderate, high)	(Increasing, stable, decreasing)
Operational				
Compliance				
Strategic				
Reputation				

2. Discuss examination findings with bank management, including violations, deficient practices, and conclusions about the corporate and risk governance structure and practices. If necessary, obtain commitments for corrective action.

3. Compose conclusion comments, highlighting any issues that should be included in the report of examination. If necessary, compose matters requiring attention and violation write-ups.

4. Update the OCC's supervisory information systems and any applicable report of examination schedules or tables.

5. Document recommendations for the supervisory strategy (e.g., what the OCC should do to effectively supervise corporate and risk governance in the bank, including time periods, staffing, and workdays required).

6. Update, organize, and reference work papers in accordance with OCC policy.

7. Appropriately dispose of or secure any paper or electronic media that contain sensitive bank or customer information.

Internal Control Questionnaire

An ICQ helps an examiner assess a bank's internal controls for an area. ICQs typically address standard controls that provide day-to-day protection of bank assets and financial records. The examiner decides the extent to which it is necessary to complete or update ICQs during examination planning or after reviewing the findings and conclusions of the core assessment.

Employee Benefits

1. Are directors or a designated committee informed at least annually of important matters relating to employee benefits, such as costs and administration problems, which would assist them in formulating any changes or modifications deemed desirable or necessary?

2. Have employee benefit plans been reviewed by bank counsel for consistency with all applicable requirements before implementation?

3. Does the bank compare its program of employee benefits with those of other banks in its peer group, and, if so, is an analysis of that comparison included in a report to the board at least annually?

4. Have all employee benefits programs currently in effect received proper board approval before the plans' inception, with appropriate documentation in the minutes?

5. Have procedures been established to confirm that all expenses related to employee benefits are correctly identified in accordance with the call report instructions and generally accepted accounting principles?

6. Are procedures in effect that call for periodic independent determinations that those individuals receiving benefits from the bank are eligible?

7. Are economies sought through the use of "standard benefits packages" that can be more efficiently administered by a bank trust department, an insurance firm, or other specialists in the industry?

8. When administration of an employee benefit plan is being handled by a third party, has the bank retained the managerial or final decision-making function about types and amounts of investments?

9. Are detailed and timely reports received that enable the bank to accurately monitor the plan?

10. Are officers and employees in sensitive positions, including personnel who have direct or indirect control of bank general ledger accounts, required to be absent for at least two consecutive weeks each year?

Conclusion

1. Is this information adequate for evaluating internal controls in that there are no significant additional internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses noted above (explain negative answers briefly, and indicate conclusions as to their effect on specific examination procedures)?

2. Based on answers to the foregoing questions, internal control for employee benefits is considered (strong, satisfactory, insufficient, or weak).

Management Information Systems

Policies or Processes

1. Has management developed and maintained MIS policies and processes?

2. Do policies and processes provide guidance in the following areas:

   - The definition, purpose, and fundamental components of MIS?
   - How to achieve effective two-way communication between management and employees and specific avenues to maintain such communication?
   - Processes for initiating, developing, and completing MIS enhancements?
   - Guidelines for installing MIS enhancements in a controlled change environment?
   - Procedures for acquiring, merging, manipulating, and uploading data to other systems?
   - Guidance for delineating the need for internal/external audit coverage and testing?

3. Are policies and processes reviewed and updated regularly?

4. Are policies and written processes distributed to appropriate employees?

5. Do policies and processes incorporate or require

   - user approval for each phase of development?
   - installation of MIS enhancements in a controlled change environment?
   - employees to follow the policy and established processes as data are acquired, merged, manipulated, and uploaded to other systems?
   - employees to be sufficiently trained for new systems and subsequent enhancements?

Development

1. Does the internal planning process consider and incorporate the importance of MIS at both the strategic and tactical level?

- Are longer-term strategic goals (beyond two years) supported by the development of appropriate MIS?
- Are shorter-term tactical goals over the immediate one- to two-year period regularly and appropriately reviewed and monitored by management?

2. Do project objectives address reported MIS weaknesses and meet business unit requirements?

3. Does management have a process for monitoring project schedules?

4. Does management use a project management technique to monitor MIS development schedules?

5. Does the bank use a consistent and standardized approach or a structured methodology for MIS projects?

6. Does the methodology encompass the following phases:

   - Analysis of the concept, organization of tasks, completions of phases, and approvals?
   - Development of the program and contracting for equipment and software?
   - Development of user manuals and testing of the system?
   - Post-review of the system and future maintenance of it?

User Training and Instructions

1. Are MIS user manuals meaningful, easy to understand, and current?

2. Do user manual requirements include the following information:

   - A brief description of the application or system?
   - Input instructions, including collection points and times to send updated information?
   - Balancing and reconciliation instructions?
   - A full listing of output reports, including samples?

Communication

1. Does management encourage communication lines to meet the following objectives:

   - To effectively link senior management, other appropriate users, and information systems employees?
   - To promote effective two-way communication between management and employees?
   - To document the MIS process?

Audit

1. Have MIS been audited according to bank's audit schedule?

   - If not, meet with audit management to determine what its plans are regarding an audit of MIS.

Conclusion

1. Is this information adequate for evaluating internal controls of MIS activities? This question presumes that there are no additional significant internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses noted above. (**Note:** Explain negative answers briefly, and indicate conclusions as to their effect on specific examination or verification procedures.)

2. Based on answers to the previous questions, internal control for MIS is considered to be (strong, satisfactory, insufficient, or weak).

Insurance

1. Does the bank have established insurance guidelines that provide for

   - a reasonably frequent, at least annual, determination of risks the bank should assume or transfer?
   - periodic appraisals of major fixed assets to be insured?
   - a credit or financial analysis of the insurance companies that have issued policies to the bank?

2. Has management established operating procedures for filing fidelity bond claims that include

   - taking prompt action when fraudulent activity is suspected to avoid further losses after what may later be regarded by the insurer as the date of discovery?
   - considering obtaining the advice and assistance of legal counsel, consultants, or accountants in filing claims?
   - ensuring adherence with insurance policy filing and notification requirements?
   - allocating human and monetary resources as warranted by the significance of the claim?
   - conducting adequate monitoring and follow-up after the claim is filed?

3. Does the bank have a risk manager who is responsible for risk control?

4. Does the bank use the services of an insurance agent or broker to assist in selecting and providing advice on alternative means of providing insurance coverage?

5. Does the bank's security officer coordinate his or her activities with the person responsible for handling the risk management function?

6. Does the bank maintain a schedule of existing insurance coverage?

7. Does the bank maintain records, by type of risk, to facilitate an analysis of the bank's experience in costs, claims, losses, and settlements under the various insurance policies in force?

8. Is a complete schedule of insurance coverage presented to the board, at least annually, for its review?

Conclusion

1. Is this information adequate for evaluating internal controls in that there are no significant additional internal auditing procedures, accounting controls, administrative controls, or other circumstances that impair any controls or mitigate any weaknesses noted above (explain negative answers briefly, and indicate conclusions as to their effect on specific examination procedures)?

2. Based on answers to the foregoing questions, internal control for indemnification and insurance is considered (strong, satisfactory, insufficient, or weak).

Verification Procedures

Verification procedures are used to verify the existence of assets and liabilities, or test the reliability of financial records. Examiners generally do not perform verification procedures as part of a typical examination. Rather, verification procedures are performed when substantive safety and soundness concerns are identified that are not mitigated by the bank's risk management systems and internal controls.

Management Information Systems

1. Using an appropriate sampling technique, select an additional MIS project(s) from the bank's development plan.

   - Review project objectives, and determine if they address reported MIS weaknesses and meet business unit plans.
   - Determine whether the MIS project(s) follow an approved and implemented development methodology that encompass the following phases:
     – Analysis of system alternatives, organization of tasks, and approval of phases by system users and owners.
     – Program development and contracts for equipment and software vendors.
     – Development of user instructions and testing the system changes.
     – Installation and maintenance of the system.

2. Using the expanded sample, check copies of relevant user instructions. Verify whether the guidelines are meaningful, easy to understand, and current.

3. Test whether user manuals provide adequate guidelines in the following areas:

   - Complete description of the system and how to use it.
   - Input instructions, including collection points and times to send updated information.
   - Reconciliation instructions.
   - Full listing of output reports, including sample formats.

4. Obtain workflows from the user manuals or managers showing data from the point-of-entry, through user processes, to final product.

   - Test the processes with users to determine if they know where the data are coming from, where data are going, and how data get there.
   - Identify the points in which data adjustments occur, if applicable.
   - Identify the individuals accountable for contributing to data and reports. Compare information with the material acquired in the step immediately preceding this step.
   - Test the preparation and reconciliation processes to verify the integrity of information.
   - Determine if data adjustments are adequately documented, if applicable.

5. Expand the sample by interviewing additional managers and experienced unit employees to determine their perceptions of MIS.

    - Discuss MIS elements of timeliness, accuracy, consistency, completeness, and relevancy.
    - Determine if the employees hold any significant perceptions that the MIS are ineffective.

6. If available, obtain samples of key senior management reports for the targeted MIS area(s). Test the following areas to determine if

    - information originates from the expected business unit.
    - users of the information are the employees one would expect and the data are being used for the correct purposes.
    - the reports are distributed to the appropriate users.

7. Review a sample of audit work papers relating to reports that disclosed material MIS weaknesses, if applicable.

    - Review documents to determine if auditors tested MIS activities against policies or practices and processes.
    - Test to determine if documented findings support the audit scope and report findings.

Appendixes

Appendix A: Board of Directors Statutory and Regulatory Requirements

National banks and FSAs are subject to certain statutory and regulatory requirements governing size, composition, and other aspects of the board and the directors. The following table highlights these requirements but does not intend to be all-inclusive, nor is it meant to be an authoritative restatement of the regulations. The regulations are subject to updates and revisions.

Table 1: Statutory and Regulatory Requirements

National banks	FSAs
Citizenship	
All national bank directors must be U.S. citizens. The OCC may waive the citizenship requirement for a minority of the total number of directors.[104]	No similar statutory or regulatory requirement.
Residency	
A majority of directors must reside in the state where the national bank is located (i.e., the state where the national bank has its main office or branches) or within 100 miles of the bank's main office for at least one year immediately preceding the election and must be a resident of the state or within 100 miles of the state.[105]	No similar statutory or regulatory requirement.
Conflicts of interest	
Although national bank directors and officers are not subject to a regulation regarding conflicts of interest, they have a fiduciary responsibility to the national bank. In addition, the common law duty of loyalty requires directors and management to act in the best interest of the national bank and to ensure insiders do not abuse their position by benefiting personally at the national bank's expense.	Directors, officers, or persons having the power to direct an FSA's management or policies or who otherwise owe a fiduciary duty to an FSA are prohibited from advancing their own personal or business interests at the expense of the FSA. Also, he or she must follow certain requirements when he or she has an interest in a matter before the board.[106]
Usurpation of corporate opportunity	
Although national bank directors and officers are not subject to a regulation regarding usurpation of corporate opportunity, they owe a common law fiduciary duty of loyalty to the bank. The usurpation of corporate opportunity doctrine, a part of the duty of loyalty, prevents insiders from improperly taking business opportunities away from the bank.	Directors, officers, or persons having the power to direct an FSA's management or policies or who otherwise owe a fiduciary duty to an FSA must not take advantage of corporate opportunities belonging to the FSA. The OCC will not deem a person to have taken advantage of a corporate opportunity belonging to the FSA if a disinterested and

[104] For more information, refer to 12 USC 72, "Qualifications."

[105] Ibid.

[106] For more information, refer to 12 CFR 163.200.

National banks	FSAs
	independent majority of the board, after receiving a full and fair presentation of the matter, rejected the opportunity as a matter of sound business judgment.[107]
Attorney	
No similar prohibition.	Not more than one director may be an attorney with a particular law firm.[108]
Stock interest	
A national bank director must own a qualifying equity interest in a national bank or a company that has control of the national bank. A minimum qualifying equity interest is common or preferred stock that has not less than an aggregate par value of $1,000, an aggregate shareholder's equity of $1,000, or an aggregate fair market value of $1,000.[109]	A director of a stock FSA need not be a stockholder of the FSA unless the bylaws so require.[110] A director of a mutual FSA is required to be a member of the FSA.[111]
President as director	
The president (but not the CEO) of the national bank is required to be a member of the board. The board may elect a director other than the president to be chair of the board.[112]	No similar statutory or regulatory requirement. Certain FSAs have bylaws, however, that require the president or CEO to be a member of the board.
Number of directors	
The number of directors of each national bank is authorized by the bylaws and limited to not less than five or more than 25, unless the OCC exempts the national bank from the 25 limit. The OCC may appoint a receiver for a national bank with fewer than five directors.[113]	The number of directors of each FSA is authorized by the bylaws and limited to not fewer than five or more than 15, unless otherwise approved by the OCC.[114]

[107] For more information, refer to 12 CFR 163.201.

[108] For more information, refer to 12 CFR 163.33, "Directors, Officers, and Employees."

[109] For more information, refer to 12 USC 72, and 12 CFR 7.2005.

[110] For more information, refer to 12 CFR 5.22(l)(1), "General Powers and Duties."

[111] For more information, refer to 12 CFR 5.21(j)(2)(viii), "Number of Directors, Membership."

[112] For more information, refer to 12 USC 76, "President of Bank as Member of Board; Chairman of Board," and 12 CFR 7.2012, "President as Director; Chief Executive Officer."

[113] For more information, refer to 12 USC 71a, "Number of Directors; Penalties"; 12 USC 191, "Appointment of Receiver for a National Bank"; and 12 CFR 7.2024, "Staggered Terms for National Bank Directors and Size of Bank Board."

[114] For more information, refer to 12 CFR 5.22(l)(2), "Number and Term," for stock associations and 12 CFR 5.21(j)(2)(viii) for mutual associations.

National banks	FSAs
Family	
No similar prohibition.	Not more than two of the directors may be members of the same immediate family.[115]
Officers or employees	
No similar statutory or regulatory requirement.	A majority of the directors must not be salaried officers or employees of the FSA or any subsidiary.[116]
Term limits	
Any national bank director may hold office for a term that does not exceed three years and until his or her successor is elected and qualified. Any national bank may adopt bylaws that provide for staggering the terms of its directors. National banks shall provide the OCC with copies of any bylaws so amended.[117]	Directors shall be elected for a term of one to three years and until their successors are elected and qualified. If a staggered board is chosen, the directors shall be divided into two or three classes as nearly equal in number as possible, and one class shall be elected by ballot annually.[118]
Committee member requirements	
Refer to the "Establish and Maintain an Appropriate Board Structure" section and appendix C of this booklet.	Refer to the "Establish and Maintain an Appropriate Board Structure" section and appendix C of this booklet.

[115] For more information, refer to 12 CFR 163.33.

[116] Ibid.

[117] For more information, refer to 12 USC 71, "Election," and 12 CFR 7.2024.

[118] For more information, refer to 12 CFR 5.22(l)(2) for stock associations and 12 CFR 5.21(j)(2)(viii) for mutual associations.

Appendix B: Regulations Requiring Board Approval for Policies and Programs

The board must approve and oversee management's implementation of written policies and certain programs and practices. The following table does not intend to be all-inclusive, nor is it meant to be an authoritative restatement of the regulations. The regulations are subject to updates and revisions.

Table 2: Regulatory Requirements

Policy	National banks and FSAs	National banks only	FSAs only
BSA compliance program	The board must approve the BSA compliance program, which establishes and maintains procedures reasonably designed to assure and monitor compliance with BSA requirements.[119]		
Compensation and employment contracts of officers, directors, and employees	Refer to the "Safe and sound banking practices" row later in this table. Also refer to the "Incentive Compensation" section of this booklet.	Officers serve at will.[120]	The board must approve all employment contracts and compensation arrangements for senior officers and directors.[121]

[119] For more information, refer to 12 CFR 21.21.

[120] For more information, refer to 12 USC 24(Fifth), "Corporate Powers of Association."

[121] For more information, refer to 12 CFR 163.39.

Policy	National banks and FSAs	National banks only	FSAs only
Fiduciary compensation and powers		A national bank may not permit any officer or employee to retain any compensation for acting as co-fiduciary with the bank in the administration of a fiduciary account, except with the specific approval of the board.[122] A national bank's asset management activities shall be managed by or under the direction of its board.[123] A national bank exercising fiduciary powers shall adopt and follow written policies and procedures adequate to maintain its fiduciary activities in compliance with applicable law.[124]	An FSA must adopt and follow written policies and procedures adequate to maintain its fiduciary activities in compliance with applicable law.[125] The exercise of fiduciary powers must be managed by or under the direction of the board.[126]
Financial derivatives		No equivalent regulation.	The board is responsible for effective oversight of financial derivative activities and must establish written policies and procedures governing such activities.[127]

[122] For more information, refer to 12 CFR 9.15(b),"Compensation of Co-Fiduciary Officers and Employees."

[123] For more information, refer to 12 CFR 9.4, "Administration of Fiduciary Powers."

[124] For more information, refer to 12 CFR 9.5, "Policies and Procedures."

[125] For more information, refer to 12 CFR 150.140, "Must I Adopt and Follow Written Policies and Procedures in Exercising Fiduciary Powers?"

[126] For more information, refer to 12 CFR 150.150, "Who Is Responsible for the Exercise of Fiduciary Powers?"

[127] For more information, refer to 12 CFR 163.172, "Financial Derivatives."

Policy	National banks and FSAs	National banks only	FSAs only
Heightened standards	Banks with average total consolidated assets of $50 billion or greater or those that are OCC-designated, which are referred to as covered banks, should have robust governance as outlined in the guidelines.[128]		
Identity theft prevention program	The board must approve the initial, written identity theft prevention program that establishes and maintains policies and procedures reasonably designed to monitor, detect, and mitigate identity theft.[129]		
Information security standards	The board or an appropriate committee of the board shall approve a written information security program and oversee the program's development, implementation, and maintenance.[130]		
Interbank liabilities	The board must review and approve written policies and procedures to prevent excessive exposure to any individual correspondent in relation to the condition of the correspondent.[131]		

[128] For more information, refer to 12 CFR 30, appendix D.

[129] For more information, refer to 12 CFR 41.90(d), "Establishment of an Identity Theft Prevention Program"; 12 CFR 41.90(e), "Administration of the Program"; and 12 CFR 41, appendix J, "Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation."

[130] For more information, refer to 12 CFR 30.

[131] For more information, refer to 12 CFR 206, "Limitations on Interbank Liabilities (Regulation F)."

Policy	National banks and FSAs	National banks only	FSAs only
Interest rate risk management	A bank should provide for periodic reporting to management and the board regarding interest rate risk with adequate information for management and the board to assess the level of risk.[132]		The board must review the association's interest rate risk exposure and devise and adopt policies for the management of interest rate risk. The board must review the results of operations at least quarterly and make appropriate adjustments as necessary.[133]
Real estate lending standards, interagency, and supplemental lending limits	A bank eligible to participate in the supplemental lending limits program for residential real estate and small business loans must submit an application to, and receive approval from, its supervisory office before using the supplemental lending limits in 12 CFR 32.7(a)(1), (2), and (3).[134]	The board must, at least annually, review and approve written policies that establish appropriate limits and standards for extensions of credit that are secured by real estate.[135]	The board must, at least annually, review and approve written policies that establish appropriate limits and standards for extensions of credit that are secured by real estate.[136]
Report of condition and income		The bank's president, a vice president, the cashier, or any other officer designated by the board must sign the report, and three directors must attest to the report's correctness.[137]	Two directors must attest to the report's correctness.[138]
Safe and sound banking practices	The board must oversee the bank's compliance with safe and sound banking practices.[139]		

[132] For more information, refer to 12 CFR 30, appendix A, II.E, "Interest Rate Exposure."

[133] For more information, refer to 12 CFR 163.176, "Interest-Rate-Risk-Management Procedures."

[134] For more information, refer to 12 CFR 32.7(b), "Application Process."

[135] For more information, refer to 12 CFR 34, subpart D, "Real Estate Lending Standards," and subpart D, appendix A, "Interagency Guidelines for Real Estate Lending."

[136] For more information, refer to 12 CFR 160.101, "Real Estate Lending Standards."

[137] For more information, refer to 12 USC 161, "Reports to Comptroller of the Currency," and 12 USC 1817(a)(3).

[138] For more information, refer to 12 USC 1464(v), "Reports of Condition," and 12 USC 1817(a)(3).

[139] For more information, refer to 12 CFR 30, "Safety and Soundness Standards."

Policy	National banks and FSAs	National banks only	FSAs only
Security program and designation of a security officer	The board must approve and oversee the adoption, implementation, and maintenance of a written security program for the main and branch offices.[140] The board must designate a security officer to report at least annually on the implementation, administration, and effectiveness of the security program.[141]		
Specific funds availability	To meet the requirements of a specific availability policy disclosure under 12 CFR 229.17 and 12 CFR 229.18(d), a bank shall provide a disclosure describing the bank's policy on when funds deposited in an account are available for withdrawal.[142]		

[140] For more information, refer to 12 CFR 30, Appendix B, III.A., "Development and Implementation of Information Security Program."

[141] For national banks, refer to 12 CFR 21, subpart A, "Minimum Security Devices and Procedures." For FSAs, refer to 12 CFR 168, "Security Procedures."

[142] For more information, refer to 12 CFR 229.16, "Specific Availability Policy Disclosure," and 12 CFR 229, appendix C, "Model Availability Policy Disclosures, Clauses, and Notices; Model Substitute Check Policy Disclosure and Notices."

Appendix C: Common Board Committees

This list provides examples of common board committees. Some committees are mandated by laws or regulations.

Table 3: Common Board Committees

Committee	Description
Executive committee	Some boards choose to use an executive committee. The executive committee generally • addresses matters requiring board review that arise between full board meetings. • relieves the full board of detailed reviews of information and operational activities. • coordinates the work of other board committees. When used, the board traditionally authorizes the executive committee to act on the board's behalf but limits the authority to exercise all of the board's powers. For example, the full board should reserve the right to execute extraordinary contracts, such as mergers and acquisitions. The full board should review the executive committee charter and verify that the charter clearly specifies the committee's authority and what the committee may approve on the board's behalf. The use of an executive committee should not lead to a two-tiered class of directors in which the executive committee wields all the power. All directors share the same responsibilities and liabilities. Additionally, the executive committee should not be confused with executive sessions of the independent directors of the board.
Audit committee	The audit committee should oversee the bank's audit program and ensure that it is sufficiently robust to identify, test, and report on all key activities in the bank. Establishing an independent audit committee to oversee and maintain the audit functions is a good, and sometimes required, practice. The bank's size and activities dictate the composition of the audit committee. The audit committee's responsibilities should include the following:[143] • Work with internal and external auditors to confirm that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities. • Hold senior management accountable for establishing and maintaining an adequate and effective internal control system and processes. • Carry out the appointment and termination, setting of compensation, and oversight of the chief auditor or equivalent and the independent public accountant or external auditor. • Ensure external auditors are independent and objective in their findings and consistent with their independence principles and rules. • Monitor the financial reporting process and oversee the bank's establishment of accounting policies and practices. • Establish and maintain whistle-blower procedures for bank employees to submit confidential and anonymous concerns for accounting, controls, or auditing matters. • Monitor, track, and hold management accountable for effectively addressing in a timely manner deficiencies that auditors or regulators identify.

[143] For more information on audit committee requirements and responsibilities, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook.*

Committee	Description
Credit committee	The credit committee oversees the bank's credit risk and its associated risk management practices. The credit committee should • establish and guide the bank's lending strategy, credit risk appetite, and risk limits. • review and approve lending policies and underwriting standards that reflect the bank's risk appetite. • approve loans as outlined in the bank's lending policy for credits involving large dollar amounts relative to the bank's size and capital levels. • monitor the loan portfolio's performance, exceptions, and the allowance for loan and lease losses. • oversee the bank's compliance with credit-related policies, limits, laws, and regulations. • receive periodic reports from the loan review function that opine on the effectiveness of the bank's loan rating systems and credit risk management practices.
Asset-liability committee	In most banks, the board delegates responsibility for overseeing liquidity and interest rate risk and its associated risk management to a committee of senior managers. If there is a board-level asset-liability committee, the committee should • establish and guide the bank's asset-liability strategies, rate risk appetites, and limits. • review liquidity and interest rate risk reports and understand key assumptions. • monitor the bank's performance and overall liquidity position and interest rate risk profile and compliance with policies, strategies, limits, and regulations. • verify that asset-liability strategies remain prudent and supported by adequate capital and liquidity levels. • identify senior managers who have authority and responsibility for managing these risks and verify that adequate resources are devoted to asset-liability management. Regulations require FSA boards to monitor financial derivatives activities and interest rate risk. FSA boards must adopt appropriate policies and procedures and periodically review them.[144] While the regulations apply only to FSAs, the guidelines contain sound practices that all banks should follow.

[144] For more information, refer to 12 CFR 163.172 and 12 CFR 163.176.

Committee	Description
Risk committee	The risk committee's primary responsibility is risk oversight. While not required, banks that have increased complexity customarily establish a separate risk committee. For smaller banks, the audit committee sometimes assumes the oversight of risk management activities. Although it is not required, larger banks often have a risk committee. The risk committee should include independent directors who review and approve a sound risk management system commensurate with the bank's size, complexity, and risk profile. The risk committee's roles and responsibilities should be explicitly defined and may include • helping to define the bank's risk appetite. • working with the board and management to confirm that the bank's strategic, liquidity, and capital plans are consistent with the bank's risk appetite statement and that material risks are addressed in the bank's risk management process. • reviewing and approving risk limits. • confirming the bank has appropriate policies and procedures for risk governance, risk management practices, and the risk control infrastructure. • working with management to establish processes for identifying and reporting risks. • addressing the bank's material risks in aggregate and by risk type. • addressing the effect of the risks to capital, earnings, and liquidity under normal and stressed conditions. • confirming the independence of the risk management functions. • overseeing and directing the work of the CRE or equivalents. • confirming effective and timely escalation of material issues to the board and holding management accountable for timely and appropriate corrective action.
	Heightened Standards The board or its risk committee should approve the risk governance framework and any significant changes.[145] The board or its risk committee also should monitor compliance with the risk governance framework.[146] Each CRE should have unrestricted access to the board risk committee regarding risk and issues identified through IRM activities.[147] The board or its risk committee approves the appointment and removal of a CRE and the CRE's annual compensation and salary adjustment.[148]

[145] For more information, refer to 12 CFR 30, appendix D, II.A.

[146] Ibid.

[147] For more information, refer to 12 CFR 30, appendix D, I.E.7, "Independent Risk Management."

[148] Ibid.

Committee	Description
Fiduciary committee	A bank with fiduciary (trust) powers must comply with a host of state and federal laws and regulations governing fiduciary activities in addition to trust accounts' governing instruments.[149] The board typically establishes three fiduciary committees to oversee fiduciary activities and asset management products and services, including fiduciary compliance: one for administrative decisions, one relating to investment oversight, and a fiduciary audit committee.[150] Smaller, less complex banks may have a variation of these committees, such as a trust committee and a fiduciary audit committee. A bank with fiduciary powers must have an audit of fiduciary activities as well as a fiduciary audit committee.[151] Regulations outline the composition requirements of the fiduciary audit committee. The committee oversees the bank's audit of significant fiduciary activities. The audit could be conducted annually or continuously, depending on the audit's setup. The committee should note results of the audit and actions taken in the minutes of the board or the fiduciary audit committee.
Compensation committee	A bank may have a compensation committee to oversee compensation arrangements. The compensation committee typically • oversees the design and implementation of any incentive compensation arrangements for covered employees as discussed in the "Oversee Compensation and Benefits Arrangements" section of this booklet. • reviews and recommends compensation for directors, including the board and board committee fee structure. • works closely with board-level risk and audit committees to confirm that all committee decisions align with the bank's strategic objectives and risk appetite, and appropriately balance risk and reward. • has an understanding of all the bank's compensation and benefits arrangements, including the relationship between the arrangements and the risks or behaviors that the arrangements may incentivize; whether the arrangements are designed to promote long-term shareholder value and not promote excessive risk taking; and the legal requirements governing such arrangements. • provides periodic reports to the full board on compensation and benefits matters. The compensation committee may assume other responsibilities, such as overseeing the bank's employee benefits plans. If the committee oversees these activities, it should confirm the bank has a process to appropriately administer benefits and meet the bank's fiduciary responsibilities. The compensation committee may engage consultants for compensation studies and assistance with developing incentive compensation arrangements. In addition, the compensation committee may be responsible for monitoring administrative costs paid to third-party professionals. If the bank has an employee benefit plan, the committee should also determine that no more than reasonable compensation is paid to the third party out of employee benefit plan assets.

[149] For more information on a national bank's fiduciary responsibilities refer to 12 CFR 9, "Fiduciary Activities of National Banks," and to the "Asset Management" booklet of the *Comptroller's Handbook*. For information on FSAs refer to 12 CFR 150, "Fiduciary Powers of Federal Savings Associations."

[150] For more information on audits of fiduciary activities, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

[151] For more information, refer to 12 CFR 9.9, "Audit of Fiduciary Activities" (national banks), and 12 CFR 150.440-480, "Audit Requirements" (FSAs).

Committee	Description
Corporate governance/ nominating committee	At many banks, the corporate governance/nominating committee duties involve • establishing criteria for board and committee membership, including qualifications and independence requirements. • recommending nominees for election to the board, evaluating new nominees, and assessing the contributions of current directors in connection with their re-nomination. • reviewing and approving a management succession policy and plan for senior management positions. • overseeing the bank's corporate governance practices with regard to board composition and independence. • verifying that the board reflects a mix of talent, expertise, and perspectives that is appropriate to the bank's needs, its strategic plans, and the overall effectiveness of the board. A mutual FSA must have a nominating committee if the association's bylaws provide for submission of nominations for directors before the annual meeting. This committee submits nominations to the secretary of the association.[152] Other responsibilities of the corporate governance/nominating committee can include • overseeing the evaluation of board performance and individual director contributions. • conducting an evaluation of its own performance. • assisting other board committees with their self-assessments. • periodically assessing board size and composition. • establishing director tenure policies that address procedures for the retirement or replacement of directors. • assessing the reporting channels and mechanisms through which the board receives information and the quality and timeliness of the information. • overseeing director education and training. • establishing and overseeing procedures for shareholder communications, including the solicitation of shareholder recommendations for the nomination of directors to the board. If the bank does not have a compensation committee to review and recommend changes to the bank's director compensation policies, the corporate governance/nominating committee should perform these duties.

[152] For more information, refer to 12 CFR 5.21(j)(2)(xiii), "Nominations for Directors."

Appendix D: Common Types of Insurance

This appendix explains some of the common types of insurance policies and coverage available to banks. The names of the insurance policies or coverage may differ among banks or providers.

Indemnification Agreements

A bank director may be named as a defendant in lawsuits that challenge his or her business decisions or activities, or allege a breach of fiduciary duty. Directors and officers, however, may obtain some protection against judgments and legal and other costs through indemnification agreements and insurance.

Banks may enter into indemnification agreements with directors. Such agreements generally provide that the bank will advance funds to, or reimburse directors for, reasonable expenses incurred in defense of legal actions. The agreement must be consistent with applicable laws and regulations and should be consistent with safe and sound banking practices.

Regulations limit indemnification agreements.[153] Banks generally may not make or agree to make indemnification payments to an institution-affiliated party (IAP) (e.g., directors, officers, employees, or controlling stockholders)[154] for liability or legal expenses resulting from administrative proceedings or civil actions instituted by any federal banking agency that results in a final order or settlement pursuant to which an IAP is

- assessed a CMP.
- removed from office or prohibited from service.
- required to cease and desist or take any described affirmative action with the bank.[155]

Reasonable indemnification payments with respect to an administrative proceeding or civil action initiated by any federal banking agency are permitted subject to the board making specific determinations and following specific procedures.[156] Reasonable indemnification payments are also permitted in other situations.[157] FSAs—but not national banks—are required to obtain OCC non-objection before making any indemnification payments.

[153] For more information, refer to 12 CFR 359.

[154] Refer to 12 USC 1813(u), "Institution-Affiliated Party," for the full definition.

[155] For more information, refer to 12 CFR 359.1(l), "Prohibited Indemnification Payment," and 12 CFR 359.3, "Prohibited Indemnification Payments."

[156] For more information, refer to 12 CFR 359.5, "Permissible Indemnification Payments."

[157] For national banks, refer to 12 CFR 7.2014, "Indemnification of Institution-Affiliated Parties." For more information regarding FSAs, refer to 12 CFR 145.121, "Indemnification of Directors, Officers and Employees."

Directors' and Officers' Liability Insurance

Director and officer (D&O) liability insurance protects directors and officers who prudently discharge their duties and helps banks attract and retain qualified personnel. D&O insurance can cover the expense of defending suits alleging director or officer misconduct, and damages that may be awarded in such lawsuits. D&O insurance can reimburse the bank for any payments made to directors or officers under an indemnification agreement. Generally, the insuring company requires a deductible for this type of coverage. This insurance does not cover criminal or dishonest acts, when involved persons obtained personal gain, or when a conflict of interest was apparent.

Insurers may add exclusionary language to insurance policies that directors and officers should clearly understand, as it has the potential to limit coverage and leave officers and directors liable for claims not covered by these policies. For instance, during times of economic slowdown, a regulatory exclusion may be added to preclude coverage for lawsuits by federal and state banking regulators. Because there is no industry standard for D&O insurance, directors should be aware of the insuring agreements and exclusions that are most critical to their personal protection. The board's choice of coverage in a D&O insurance policy should be based on a well-informed analysis of the cost and benefits, and the potential impact that could result from exclusions. When considering renewals and amendments to existing policies, directors and officers should consider the following:

- What protections do I want from my bank's D&O insurance policy?
- What exclusions exist in my bank's D&O insurance policy?
- Are any of the exclusions new, and, if so, how do they change my D&O insurance coverage?
- What is my potential personal financial exposure arising from each D&O insurance policy exclusion?

D&O liability insurers have filed suits to rescind coverage against directors and officers in cases involving restatement of financials or other alleged financial misconduct. The insurers typically claim that the policy should be rescinded on the grounds that it was fraudulently procured. Directors and officers may consider a clean non-rescindable clause, providing that the insurer cannot rescind the policy based on alleged corporate wrongdoing or misrepresentations in the application process. Such a clause is generally not included in standard policies, and insurers charge a significant premium for its inclusion.

The severability clause of the D&O policy generally provides that no knowledge or statement by anyone insured in procuring coverage can be imputed to any other insured individual, limiting the potential that coverage will be adversely affected for one individual as the result of the actions of another. The practical effect of the severability clause is to require an insurer seeking to rescind a policy to prove knowledge of each insured person separately. Narrowly tailored severability clauses may limit the insurer's potential exposure.

Refer to the "Indemnification Agreements" section of this booklet for the instances in which the bank may and may not purchase D&O insurance to pay or reimburse an IAP.

Fidelity Bond

Fidelity insurance includes reimbursement for loss, not only from employee dishonesty but also from robbery, burglary, theft, forgery, mysterious disappearance, and, in specified instances, damage to offices or fixtures of the insured. Fidelity bond coverage applies to all banking locations except automated teller machines, for which coverage must be specifically added by a rider. Standard procedure for insurance companies is to write fidelity bonds on a "discovery" basis. Under this method, the insurance company is liable up to the full amount of the policy for losses covered by the terms of the bond and discovered while the bond is in force, regardless of the date on which the loss was actually sustained by the bank. This procedure applies even though lower coverage amounts or more restrictive terms might have been in effect on the date the loss was sustained.

All fidelity bonds require that a loss be reported to the bonding company within a specified time after a reportable item comes to the attention of management. Management should diligently report all potential claims to the bank's insurance company because failure to file a timely report may jeopardize coverage for that loss.

Many banks also obtain an excess coverage policy. The coverage extends the basic protection provided under the fidelity bond in areas in which the dollar volume of assets or exposure is particularly high. Fidelity bond protection can be extended by purchasing optional riders.

If the bank discontinues efforts to obtain insurance after the policy lapses or is canceled, the board should be aware that

- the failure of directors to require bonds with adequate sureties and in sufficient amounts may make the directors personally liable for any losses the bank sustains because of the absence of such bonds. Common law standards have held directors liable in their "personal and individual capacity" for negligently failing to require an indemnity bond to cover employees with access to cash, notes, and securities.
- management should determine the reason for any denial of insurance or unreasonable terms; confirm that action is taken to correct any deficiencies and, when beneficial, provide additional information; and obtain insurance when feasible.
- although establishing a fund to cover losses is not a viable alternative to insurance, it may be used while attempting to obtain insurance (to be applied to premiums or to offset losses), or it may be used in addition to insurance to offset a high deductible. Establishing such a fund does not mean that an insurance cost or liability has been incurred. Therefore, estimated losses should not be reported as an expense in the call report until the losses actually occur.

When the bank is a subsidiary of a bank holding company, and the holding company has purchased one fidelity bond to cover all affiliated banks, the bank should be careful when determining that the policy is sufficient to cover the bank's exposures.

Bank-Owned Life Insurance

Bank-owned life insurance (BOLI) is a form of life insurance purchased by banks in which the bank is the beneficiary or owner. This form of insurance is a tax shelter for the administering bank. The cash flows from a BOLI policy generally are income tax-free if the bank holds the policy for its full term. Banks are not authorized to purchase BOLI as an investment. BOLI can, however, provide attractive tax-equivalent yields to help offset the cost of employee benefits. Banks are expected to establish sound risk management processes, including meaningful risk limits, before implementing and adding to a BOLI program.[158]

Specialized Bank Insurance

Management, in consultation with the board, may decide that they should obtain other bank insurance coverage to transfer risks. The following are some of the most frequently purchased types of specialized bank insurance:

Automobile, public liability, and property damage: Protects against property and liability losses arising from injury or death when a bank-owned, -rented, or -repossessed vehicle is involved. Non-ownership liability insurance should be considered if officers or employees use their own cars for bank business.

Boiler and machinery: Provides coverage for loss due to explosion or other forms of destruction of boilers, heating or cooling systems, and similar types of equipment.

Business disruption expense: Provides funds for the additional costs of reestablishing the bank's operations after a disaster.

Combination safe depository, coverage A: Covers losses when the bank is legally obligated to pay for the loss (including damage or destruction) of a customer's property held in safe deposit boxes. **Coverage B:** Covers loss, damage, or destruction of property in customers' safe deposit boxes, whether or not the bank is legally liable, when such loss results from activities other than employee dishonesty. This policy commonly provides for reimbursement of legal fees in conjunction with defending suits involving alleged loss of property from safe deposit boxes.

Cybersecurity: Provides coverage to mitigate losses for a variety of cyber incidents, including data breaches, business interruption, and network damage.

Fine arts: Provides coverage for works of art on display at a bank, whether owned by the bank or on consignment. Protection typically is all risk and requires that appraisals of the objects be made regularly to establish the insurable value.

Fire: Covers all loss directly attributed to fire, including damage from smoke, water, or chemicals used to extinguish the fire. Additional fire damage for the building contents may

[158] For more information, refer to OCC Bulletin 2004-56, "Bank-Owned Life Insurance: Interagency Statement on the Purchase and Risk Management of Life Insurance."

be included but often is written in combination with the policy on the building and permanent fixtures. Most fire insurance policies contain "co-insurance" clauses, meaning that insurance coverage should be maintained at a fixed proportion of the replacement value of the building.

First class, certified, and registered mail insurance: Provides protection on shipment of property sent by various types of mail and during transit by messenger or carrier to and from the U.S. Postal Service. This coverage is used principally for registered mail over the maximum $25,000 insurance provided by the U.S. Postal Service.

Fraudulent accounts receivable and fraudulent warehouse receipts: Covers losses resulting from the pledging of fraudulent or nonexistent accounts receivable and warehouse receipts, or from situations in which the pledger does not have title. In addition, this insurance offers protection against loss arising from diversion of proceeds through acts of dishonesty.

General liability: Covers possible losses arising from a variety of occurrences. General liability insurance provides coverage against specified hazards, such as personal injury, medical payments, landlords' or garage owners' liability, or other specific risks that may result in or create exposure to a suit for damages against the bank. "Comprehensive" general liability insurance covers all risks, except specific exclusions.

Key person insurance: Insures the bank on the life of an officer when the death of such officer, or key person, would be of such consequence as to give the bank an insurable interest.

Mortgage errors and omissions: Protects the bank, as mortgagee, from loss when fire or all-risk insurance on real property held as collateral inadvertently has not been obtained. This insurance is not intended to overcome errors in judgment, such as inadequate coverage or insolvency of an original insurer.

Single interest: Covers losses for uninsured vehicles that are pledged as collateral for an extension of credit.

Transit cash letter insurance: Covers loss of cash letter items in transit for collection or to a clearinghouse of which the insured bank is a member. This coverage also includes costs for reproducing cash letter items. Generally, such coverage does not include items sent by registered mail or air express or losses due to dishonest acts of employees.

Trust operations errors and omissions: Indemnifies against claims for damages arising from alleged acts resulting from error or omissions while acting as administrator under a trust agreement.

Umbrella liability: Provides excess coverage over existing liability policies, as well as basic coverage for most known risks not covered by existing insurance.

Valuable papers and destruction of records: Covers cost of reproducing records damaged or destroyed. This coverage also includes the cost of research needed to develop the facts required to replace books of accounts and records.

Appendix E: Glossary

Control functions: Those functions that have a responsibility to provide independent and objective assessment, reporting, and assurance. They include the risk review, compliance, and internal audit functions.

Corporate governance: A set of relationships among a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and by which the means of attaining those objectives and monitoring performance are determined.

Credible challenge: The method that directors use to hold management accountable by being engaged and asking questions and eliciting any facts necessary, when appropriate, to satisfy themselves that management's strategies are viable and in the bank's best interests.

Duty of care: The duty of a board member to decide and act in an informed and prudent manner with respect to the bank. Often interpreted as requiring a board member to approach the affairs of the company the same way that a "prudent person" would approach his or her own affairs.

Duty of loyalty: The duty of a board member to act in good faith in the interest of the company. The duty of loyalty should prevent an individual director from acting in his or her own interest, or in the interest of another individual or group, at the expense of the company and all shareholders.

Independent director: A director is viewed as independent if he or she is free of any family relationship or any material business or professional relationship (other than stock ownership and the directorship itself) with the bank, its holding company, its affiliate, or its management.

Management director: A member of the board (such as a director) who also has management responsibilities within the bank.

Risk appetite statement: The written statement of the aggregate level and types of risk that a bank is willing to assume to achieve its strategic objectives and business plan. It includes quantitative measures expressed relative to earnings, capital, risk measures, liquidity, and other relevant measures as appropriate. It should include qualitative statements to address reputation risk as well as money laundering and unethical practices.

Risk culture: The bank's norms, attitudes, and behaviors related to risk awareness, risk taking, and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during day-to-day activities and affects the risks they assume.

Risk governance framework: A part of the corporate governance framework, through which the board and management, in their respective roles, establish and make decisions

about the bank's strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits consistent with the bank's strategy; and identify, measure, monitor, and control risks.

Risk limits: Specific quantitative measures based on, for example, forward-looking assumptions that allocate the bank's risk appetite to business lines; legal entities as relevant, specific risk categories; concentrations; and, as appropriate, other measures.

Risk management: The processes established to identify, measure, monitor, and control material risks and associated risk concentrations.

Risk profile: Point-in-time assessment of the bank's risks, aggregated within and across each relevant risk category based on current and forward-looking assumptions.

Appendix F: Abbreviations

AML	anti-money laundering
BOLI	bank-owned life insurance
BSA	Bank Secrecy Act
CAE	chief audit executive
CAMELS	capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk
CEO	chief executive officer
CFR	Code of Federal Regulations
CIO	chief information officer
CISO	chief information security officer
CMP	civil money penalty
CMS	compliance management system
COO	chief operating officer
CRA	Community Reinvestment Act
CRE	chief risk executive
CTO	chief technology officer
D&O	director and officer
EIC	examiner-in-charge
ERM	enterprise risk management
Fed. Reg.	Federal Register
FFIEC	Federal Financial Institutions Examination Council
FSA	federal savings association
IAP	institution-affiliated party
ICQ	internal control questionnaire
IRM	independent risk management
IT	information technology
MIS	management information systems
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
ROCA	risk management, operational controls, compliance, and asset quality
USC	U.S. Code

References

Listed references apply to national banks and FSAs unless otherwise noted.

Laws

12 USC 24(Fifth), “Corporate Powers of Association” (national banks)
12 USC 61, “Shareholders' Voting Rights; Cumulative and Distributive Voting; Preferred Stock; Trust Shares; Proxies, Liability Restrictions; Percentage Requirement Exclusion of Trust Shares” (national banks)
12 USC 71, “Election” (national banks)
12 USC 71a, “Number of Directors; Penalties” (national banks)
12 USC 72, “Qualifications” (national banks)
12 USC 73, “Oath” (national banks)
12 USC 74, “Vacancies” (national banks)
12 USC 76, “President of Bank as Member of Board; Chairman of Board” (national banks)
12 USC 161, “Reports to Comptroller of the Currency” (national banks)
12 USC 191, “Appointment of Receiver for a National Bank” (national banks)
12 USC 371c, “Banking Affiliates”
12 USC 1464(v), “Reports of Condition” (FSAs)
12 USC 1813(u), “Institution-Affiliated Party”
12 USC 1817(a), “Reports of Condition; Access to Reports”
12 USC 1817(j), “Change in Control of Insured Depository Institutions”
12 USC 1818, “Termination of Status as Insured Depository Institution”
12 USC 1828(z), “General Prohibition on Sale of Assets”
12 USC 1831i, “Agency Disapproval of Directors and Senior Executive Officers of Insured Depository Institutions or Depository Institution Holding Companies”
12 USC 1831o, “Prompt Corrective Action”
12 USC 2901 et seq., “Community Reinvestment”
12 USC 3201 et seq., “Depository Institution Management Interlocks”
15 USC 45, “Unfair Methods of Competition Unlawful; Prevention by Commission”
15 USC 77jjj, “Eligibility and Disqualification of Trustee”
15 USC 1691(a), “Activities Constituting Discrimination”
18 USC 215, “Receipt of Commissions or Gifts for Procuring Loans”
18 USC 656, “Theft, Embezzlement, or Misapplication by Bank Officer or Employee”
18 USC 1001, “Statements or Entries Generally”
18 USC 1005, “Bank Entries, Reports, and Transactions”
18 USC 1344, “Bank Fraud”
29 USC 1001 et seq., “Employee Retirement Income Security Program”
31 USC 5322, “Criminal Penalties”
42 USC 3604, “Discrimination in the Sale or Rental of Housing and Other Prohibited Practices”
42 USC 3605, “Discrimination in Residential Real Estate-Related Transactions”
52 USC 30101 et seq., “Federal Election Campaign Act of 1971”

Regulations

11 CFR 100, subpart B, "Definition of Contribution"
11 CFR 114.2, "Prohibitions on Contributions, Expenditures and Electioneering Communications"
12 CFR 3, "Capital Adequacy Standards"
12 CFR 5.21, "Federal Mutual Savings Association Charter and Bylaws" (mutual FSAs)
12 CFR 5.22, "Federal Stock Savings Association Charter and Bylaws" (stock FSAs)
12 CFR 5.23, "Conversion to Become a Federal Savings Association" (FSAs)
12 CFR 5.24, "Conversion to Become a National Bank" (national banks)
12 CFR 5.40, "Change in "ocation of a Main Office of a National Bank or Home Office of a Federal Savings Association"
12 CFR 5.46, "Changes in Permanent Capital of a National Bank" (national banks)
12 CFR 5.50, "Change in Control of a National Bank or Federal Savings Association; Reporting of Stock Loans"
12 CFR 5.51, "Changes in Directors and Senior Executive Officers of a National Bank or Federal Savings Association"
12 CFR 7.2002, "Director or Attorney as Proxy" (national banks)
12 CFR 7.2004, "Honorary Directors or Advisory Boards" (national banks)
12 CFR 7.2005, "Ownership of Stock Necessary to Qualify as Director" (national banks)
12 CFR 7.2007(a), "Increasing Board of Directors" (national banks)
12 CFR 7.2008, "Oath of Directors" (national banks)
12 CFR 7.2009, "Quorum of the Board of Directors; Proxies Not Permissible" (national banks)
12 CFR 7.2012, "President as Director; Chief Executive Officer" (national banks)
12 CFR 7.2014, "Indemnification of Institution-Affiliated Parties" (national banks)
12 CFR 7.2024, "Staggered Terms for National Bank Directors and Size of Bank Board" (national banks)
12 CFR 9, "Fiduciary Activities of National Banks" (national banks)
12 CFR 11, "Securities Exchange Act Disclosure Rules"
12 CFR 21, subpart A, "Minimum Security Devices and Procedures" (national banks)
12 CFR 21.11, "Suspicious Activity Report" (national banks)
12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act Compliance"
12 CFR 25, "Community Reinvestment Act and Interstate Deposit Production Regulations" (national banks)
12 CFR 26, "Management Official Interlocks"
12 CFR 30, "Safety and Soundness Standards"
12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"
12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards"
12 CFR 30, appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches"

12 CFR 30, appendix E, “OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches”
12 CFR 31, “Extensions of Credit to Insiders and Transactions With Affiliates”
12 CFR 32.7, “Residential real estate loans, small business loans, and small farm loans ('Supplemental Lending Limits Program')”
12 CFR 34, subpart D, “Real Estate Lending Standards” (national banks)
12 CFR 34.62, subpart D, appendix A, “Interagency Guidelines for Real Estate Lending” (national banks)
12 CFR 41.90, “Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft”
12 CFR 41, appendix J, “Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.”
12 CFR 145.121, “Indemnification of Directors, Officers and Employees” (FSAs)
12 CFR 150, “Fiduciary Powers of Federal Savings Associations” (FSAs)
12 CFR 160.101, “Real Estate Lending Standards” (FSAs)
12 CFR 160.101, appendix, “Interagency Guidelines for Real Estate Lending Policies” (FSAs)
12 CFR 163.33, “Directors, Officers, and Employees” (FSAs)
12 CFR 163.39, “Employment Contracts” (FSAs)
12 CFR 163.172, “Financial Derivatives” (FSAs)
12 CFR 163.176, “Interest-Rate-Risk-Management Procedures” (FSAs)
12 CFR 163.180(d), “Suspicious Activity Reports” (FSAs)
12 CFR 163.200, “Conflicts of Interest” (FSAs)
12 CFR 163.201, “Corporate Opportunity” (FSAs)
12 CFR 168, “Security Procedures” (FSAs)
12 CFR 195, “Community Reinvestment” (FSAs)
12 CFR 206, “Limitations on Interbank Liabilities (Regulation F)”
12 CFR 215, “Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (Regulation O)”
12 CFR 223, “Transactions Between Member Banks and Their Affiliates (Regulation W)”
12 CFR 225.41(b)(3), “Immediate Family”
12 CFR 229, “Availability of Funds and Collection of Checks (Regulation CC)”
12 CFR 359, “Golden Parachute and Indemnification Payments”
12 CFR 363, “Annual Independent Audits and Reporting Requirements”
12 CFR 1026.36, “Prohibited Acts or Practices and Certain Requirements for Credit Secured by a Dwelling”
31 CFR 1020.210, “Anti-Money Laundering Program Requirements for Financial Institutions Regulated Only by a Federal Functional Regulator, Including Banks, Savings Associations, and Credit Unions”

Federal Register

83 Fed. Reg. 66604

Comptroller's Handbook

"Asset Management"
"Bank Supervision Process"
"Capital and Dividends"
"Community Bank Supervision"
"Community Reinvestment Act Examination Procedures" (national banks)
"Compliance Management Systems"
"Federal Branches and Agencies Supervision"
"Insider Activities"
"Internal and External Audits"
"Internal Control" (national banks)
"Large Bank Supervision"
"Liquidity"
"Recovery Planning"
"Related Organizations" (national banks)
"Retirement Plan Products and Services"

OTS Examination Handbook (FSAs)

Section 1500, "Community Reinvestment Act"
Section 340, "Internal Control"
Section 730, "Related Organizations"

Comptroller's Licensing Manual

"Background Investigations"
"Change in Bank Control"
"Changes in Directors and Senior Executive Officers"
"Charters"
"Conversions to Federal Charter"

OCC Issuances

Detecting Red Flags in Board Reports: A Guide for Directors
OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing"
OCC Bulletin 2004-56, "Bank-Owned Life Insurance: Interagency Statement on the Purchase and Risk Management of Life Insurance"
OCC Bulletin 2007-31, "Prohibition on Political Contributions by National Banks: Updated Guidance"
OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies"
OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"
OCC Bulletin 2014-35, "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations"

OCC Bulletin 2015-30, "Standards for Assessing the Diversity Policies and Practices of Regulated Entities: Final Interagency Policy Statement"
OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles"
OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"
OCC Bulletin 2018-17, "Supervisory Policy and Processes for Community Reinvestment Act Performance Evaluations"
The Director's Book: Role of Directors for National Banks and Federal Savings Associations

Other

Basel Committee on Banking Supervision's "Principles for Effective Risk Data Aggregation and Risk Reporting," January 2013
FFIEC BSA/AML Examination Manual
FFIEC IT Examination Handbook