Office of the
Comptroller of the Currency

RESCINDED

The Director's Book

Role of Directors for National Banks and Federal Savings Associations

This booklet is replaced by version 2.0 of the booklet of the same title published November 2020.

This page intentionally left blank

RESCINDED

The Director's Book

Role of Directors for National Banks and Federal Savings Associations

July 2016

Office of the Comptroller of the Currency

This page intentionally left blank

Contents

Preface

The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises all national banks and federal savings associations (collectively, banks), as well as federal branches and agencies of foreign banks. In regulating banks, the OCC has the power to

- examine the banks.
- approve or deny applications for new charters, branches, capital, or other changes in corporate or banking structure.
- take supervisory actions against banks that do not comply with laws and regulations or that otherwise engage in unsafe or unsound practices. The OCC also can remove officers and directors, negotiate agreements to change banking practices, and issue cease-and-desist (C&D) orders as well as civil money penalties (CMP).
- issue rules and regulations, legal interpretations, and corporate decisions governing investments, lending, and other activities.

Boards of directors play critical roles in the successful operation of banks. The OCC recognizes the challenges facing bank directors. *The Director's Book: Role of Directors for National Banks and Federal Savings Associations* helps directors fulfill their responsibilities in a prudent manner. This book provides an overview of the OCC, outlines directors' responsibilities as well as management's role, explains basic concepts and standards for safe and sound operation of banks, and delineates laws and regulations that apply to banks. To better understand a particular bank activity and its associated risks, directors should refer to the *Comptroller's Handbook* booklets, including the "Corporate and Risk Governance" booklet. For information generally found in board reports, including "red flags"—ratios or trends that may signal existing or potential problems—directors should refer to *Detecting Red Flags in Board Reports: A Guide for Directors*.

The OCC published *The Director's Book* in 1987 and revised it in 1997 and 2010. This 2016 edition reflects legal and regulatory changes since 2010. Changes include the transfer of regulatory and supervisory authority for federal savings associations (FSA) to the OCC pursuant to the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010. When it is necessary to distinguish between national banks and FSAs, they are referred to separately in this book.

This book does not create rights or legal protections for banks or directors, nor does it create obligations for the OCC. Directors should review their responsibilities, continuously assess their conduct, and seek advice from legal counsel when necessary.

For purposes of this book, the term "board" refers to the board of directors or a designated committee thereof unless otherwise stated. The term "senior management" refers to bank employees designated by the board as executives responsible for making key decisions. Senior management may include, but is not limited to, the president, chief executive officer (CEO), chief financial officer, chief risk executive (CRE),[1] chief information officer (CIO), chief compliance officer, chief credit officer, chief auditor, and chief bank counsel. Titles and positions vary depending on the bank's structure, size, and complexity. Unless otherwise noted, the book uses the terms "CEO" and "president" to refer to the individual 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.

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

OCC Supervisory Activities

Banking is essentially a business of assuming and managing risk. The OCC's bank supervision process is designed to ensure that banks operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations.

The OCC employs a risk-based supervisory philosophy focused on evaluating a bank's risk, identifying material and emerging problems, and ensuring that appropriate individuals at banks take corrective action before problems compromise the bank's safety and soundness. This philosophy is embodied in the OCC's supervision-by-risk program. The OCC carries out risk-based supervision for safety and soundness purposes, including in specialty areas such as information technology (IT), asset management, and consumer compliance.

Supervision by risk consists of determining the quantity of a bank's risk and evaluating the quality of risk management systems to control risk. The supervision process also assesses the aggregate level of risk and the direction of risk for the eight OCC-defined categories of risk: credit, interest rate, liquidity, price, operational compliance, strategic, and reputation. Supervision by risk provides consistent risk identification, a structure for assessing these risks, and integration of the risk assessment in the supervisory process. Supervision by risk places the responsibility for controlling risks with the board and management. The OCC assesses how well a bank manages its risks over time, rather than assessing only the condition at a single point in time. For more information about the categories of risk and the supervision by risk program, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook.*

The OCC supervises banks by conducting full-scope and targeted examinations and ongoing monitoring. These activities help determine the condition of individual banks and the overall stability of the banking system. The OCC and other federal bank regulatory agencies use the Uniform Financial Institutions Rating System, or CAMELS, to assign the composite and component ratings to banks.[2] The OCC assigns ROCA[3] ratings for federal branches and agencies of foreign banking organizations. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for more information about the CAMELS and ROCA rating systems. The composite and component ratings disclosed in written communication to the bank are subject to the confidentiality rules imposed by 12 CFR 4. The OCC also

---

2 A bank's composite CAMELS rating integrates ratings from six component areas: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk. Bank Secrecy Act/anti-money laundering examination findings in a safety and soundness context are included as part of the management component. The ratings range from 1 to 5 with 1 being the highest rating and least supervisory concern.

3 ROCA is an interagency uniform supervisory rating system for branches and agencies of foreign banking organizations that assesses risk management, operational controls, compliance, and asset quality.

evaluates the bank's risk profile through its risk assessment system. The OCC establishes its supervisory strategies based on a bank's size, complexity, risk profile, and condition. Generally, the OCC is required to conduct examinations annually, although 18-month cycles are permitted for smaller, lower-risk institutions.[4]

The OCC uses other systems to assign ratings to specific aspects of a bank's activities. These include the Uniform Rating System for Information Technology, which assesses bank and service provider risks introduced by IT; the Uniform Interagency Trust Rating System, which evaluates the bank's fiduciary activities; and the Uniform Interagency Consumer Compliance Rating System, which reflects, in a comprehensive and uniform fashion, the nature and extent of a bank's compliance with consumer protection and regulations. Separately, the OCC assigns a rating for the bank's record of performance under the Community Reinvestment Act (CRA) and compliance with regulations implementing the CRA. Refer to the "Bank Supervision Process booklet" of the *Comptroller's Handbook* for more information about these rating systems.

The OCC has two departments that provide supervisory and regulatory oversight of banks: Midsize and Community Bank Supervision (MCBS) and Large Bank Supervision (LBS). Many factors determine whether MCBS or LBS supervises a bank, including business model, strategic initiatives, asset size, and complexity as well as designation by OCC senior management. As a general rule, however, banks in the community bank portfolio range from de novo (newly chartered) to those having total assets up to $10 billion. The midsize portfolio generally has banks with total assets—either in a single charter or aggregated among several charters—greater than $10 billion and up to $100 billion. The large bank portfolio comprises the largest, most complex companies, generally with more than $100 billion in total assets. The LBS program also includes most foreign-owned banks and federal branches and agencies of foreign banks.

The OCC's Community Bank Supervision program, which is part of MCBS, is centered on local field offices using a portfolio management approach. An OCC portfolio manager is assigned to each community bank and tailors the supervision of each bank to its individual risk profile, business model, and management strategies. The Community Bank Supervision program ensures that community banks receive the benefits of highly trained bank examiners with local knowledge and experience, along with the resources and specialized expertise that a nationwide perspective can provide. OCC examiners meet with community bank management during an examination to obtain information or discuss issues. When the examination is complete, examiners prepare a report of examination and meet with the bank's board (except for some smaller affiliates of larger banks, in which case the meeting may be conducted with the lead bank's board) to discuss the results of the

---

[4] For more information, refer to 12 USC 1820(d), "Annual On-Site Examinations of All Insured Depository Institutions Required"; 12 CFR 4.6, "Frequency of Examination of National Banks and Federal Savings Associations"; and 12 CFR 4.7, "Frequency of Examination of Federal Agencies and Branches."

examination. Each director is responsible for thoroughly reviewing and signing the report of examination. The "Community Bank Supervision" booklet of the *Comptroller's Handbook* and *A Common Sense Approach to Community Banks* provide more information about the OCC's supervision of smaller institutions.

The OCC's Midsize Bank Supervision program, which is part of MCBS, provides effective, risk-based continuous supervision of complex midsize banks with diversified business models. Banks in this portfolio operate in multiple states and regions, and the banks typically lead market share in these geographies. The scope and complexity of the operations of midsize banks require full-time examiners-in-charge (EIC) to provide effective continuous supervision. A designated EIC is assigned to each bank, as are functional EICs for each key risk area. The midsize program allows Midsize Bank Supervision to provide a national perspective balanced with a local presence; subject matter expertise; and continuity in supervision because the EICs and their respective teams possess strong institutional knowledge of key issues and risk.

The OCC's LBS program provides continuous, on-site, risk-based supervision through a team of examiners assigned to each large bank, which are led by a designated EIC. The resident examiners are assigned to a risk area and are responsible for conducting both ongoing supervision of their assigned areas and targeted examinations. Banks in this portfolio are the largest and most complex in the federal banking system and often operate globally. Many large banks are also part of diversified financial organizations. Therefore, the LBS program assesses the risks posed by related entities as well. This approach recognizes that risks present in a bank may be mitigated or increased by activities in an affiliate. The LBS program enables the OCC to maintain an ongoing program of risk assessment, monitoring, and communication with bank management and directors. The program is structured to provide rigorous, informed, and consistent supervision across large banks. The "Large Bank Supervision" booklet of the *Comptroller's Handbook* provides more information about the OCC's supervision of large banks.

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 adhere 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" (referred to in this book as heightened standards).

Heightened Standards
Specific criteria for covered banks, subject to 12 CFR 30, appendix D, are noted in text boxes like this one throughout this book.

The OCC's supervisory authority is not limited to the bank itself. As the primary regulator of national banks and FSAs, the OCC also has authority over bank subsidiaries, including the authority to examine, require reports from, and take other actions against these subsidiaries.[5] Further, the OCC has the authority to examine affiliates.[6] In addition, the OCC generally has the authority to examine and regulate functions or operations performed for or provided to the bank by third parties to the same extent as if they were performed by the bank itself on its own premises.[7]

The OCC promotes open communication between examiners and board members of a bank. OCC examiners have experience with a broad range of banking activities and can provide independent, objective advice on safe and sound banking principles and compliance with laws and regulations.[8] Establishing and maintaining open and regular communications with the supervisory agencies helps the board and management properly interpret expectations for risk management and governance and apply them to normal duties and responsibilities.

Directors are encouraged to meet with OCC examiners to discuss the condition of the bank and the results of the examination. Independent directors also are encouraged to meet with OCC examiners without management's presence. Directors should pay close attention to and review carefully any written communications from the OCC. They should ask questions and raise issues of concern. Directors need to satisfy themselves that management's relations with the OCC are effective, management treats compliance issues and supervisory findings seriously, and management completes any specific follow-up actions promptly.

The activities of OCC examiners in no way diminish the board's responsibilities to oversee the management and operation of the bank. Directors are independently responsible for knowing the condition of the bank and should not rely on the examiners as their sole source of information to identify or correct problems. Instead, the board should look to its senior management, its auditors, and other independent experts to identify and correct any problems.

To understand bank issues, each director should personally review all reports and significant communications from the bank's auditors and regulators.

---

5 The Gramm–Leach–Bliley Act (GLBA) limited the OCC's authority over bank affiliates and subsidiaries regulated by or registered with the U.S. Securities and Exchange Commission, the U.S. Commodity Futures Trading Commission, and state insurance commissioners (functionally regulated affiliates). The GLBA imposed strict limits on the OCC's authority to examine, require reports from, impose capital requirements on, and take direct or indirect actions against such entities. Dodd–Frank, however, later modified or removed many, but not all, of these limits, restoring much of the authority the OCC had over functionally regulated affiliates before the GLBA. For more information on the OCC's authority over such entities, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook*.

6 For more information on national banks, refer to 12 USC 481, "Appointment of Examiners; Examination of Member Banks, State Banks, and Trust Companies; Reports." For FSAs, refer to 12 USC 1464(d)(1)(B), "Ancillary Provisions."

7 For more information, refer to 12 USC 1867(c), "Services Provided by Contract or Otherwise," and 12 USC 1464(d)(7), "Regulation and Examination of Savings Association Service Companies, Subsidiaries, and Service Providers."

8 The OCC does not provide legal advice to banks or board members. Banks and board members should consult their own legal counsel for legal advice.

Information from these reviews can help the entire board assess the accuracy and validity of information from management. A director who needs help understanding the findings or recommendations of a report should contact the regulator, the bank's audit committee,[9] auditors, or independent consultants who prepared the report.

Regulatory and other reports, such as independent risk management (IRM) or internal audit reports, also inform directors of the deficiencies within the bank. Directors must understand all identified concerns and problems and confirm that management executes sustainable corrective actions within specified time frames. Uncorrected supervisory concerns contained in matters requiring attention (MRA) or enforcement action articles resulting from the board's failure to supervise the bank appropriately may result in the OCC's holding individual directors accountable for the lack of corrective action.[10]

At the close of an examination or other supervisory activity, the examiners provide the bank's board and management with a report of examination or other communication that identifies any MRAs. MRAs describe practices that

- deviate from sound governance, internal control, and risk management principles, and have the potential to adversely affect the bank's condition, including its financial performance or risk profile, if not addressed.
- result in noncompliance with laws and regulations, enforcement actions, supervisory guidance, or conditions imposed in writing in connection with the approval of any application or other request by the bank.

MRAs require timely and effective corrective action by the bank's board and management. The communication describes the concern(s) and identifies the root cause(s) of the concern and contributing factors. The MRA also describes potential consequences or effects on the bank if actions are not taken, and supervisory expectations for corrective actions. Finally, the MRA documents management's commitments to corrective action and includes the time frames and the persons responsible for corrective action.

The corrective action for an MRA is mandatory. Bank management must develop a corrective action plan to avoid an enforcement action.

The board must approve the plan. The OCC also expects the board to

- hold management accountable for the deficient practices.
- direct management to develop and implement corrective actions.
- approve the necessary changes to the bank's policies, processes, procedures, and controls.
- establish processes to monitor progress and verify and validate the effectiveness of management's corrective actions.

---

9 For more information about the audit committee, refer to the "Audit Committee" section of this book.

10 For more information, refer to the "Actions Against Individuals" section of this book.

For more information on MRAs, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* and OCC Bulletin 2014-52, "Matters Requiring Attention: Updated Guidance."

Resources

OCC Resources

The OCC has responded to the need of banks and their directors for more practical information and tools that can help them identify and respond to emerging risks and keep track of new or changing regulatory and supervisory requirements.

A primary tool for directors and management is BankNet, the OCC's secure website for communicating with and receiving information from national banks and FSAs. BankNet, which is available only to OCC-regulated banks, not to the public, contains information that is not obtainable elsewhere. The site contains features, tools, applications, services, and information that are useful to bankers and directors in meeting their regulatory responsibilities and information needs. Resources to BankNet subscribers include capital estimation and stress-testing tools that help directors compare a bank's performance with a custom peer group and established benchmarks. BankNet delivers accurate, timely, and confidential data on a secure platform that ensures both information security and data integrity.

The OCC also provides other resources on the OCC's website. Bankers and directors can subscribe to OCC news e-mail listservs and RSS feeds to receive OCC alerts, bulletins, news releases, public service podcasts, and *SuperVisions* newsletters. In addition, the OCC engages in substantial outreach to bankers and bank directors, including the director workshops held throughout the year that focus on the fundamentals of being a director as well as hot topics and critical updates. Further, directors have access to highly trained OCC staff, including the lead experts and policy analysts, as well as the OCC's legal and licensing staffs.

Other Resources

The board may need to contact federal bank regulatory agencies other than the OCC, namely, the Board of Governors of the Federal Reserve System (Federal Reserve Board), the Federal Deposit Insurance Corporation (FDIC), and the Consumer Financial Protection Bureau. The following table summarizes the primary and secondary supervisory responsibilities of the three prudential bank regulatory agencies—the OCC, the Federal Reserve Board, and the FDIC. The table also shows that these agencies' jurisdictions sometimes overlap. When this occurs, the agencies work together and share information to reduce the burden to both the bank and the agencies.

Bank regulatory agency	Prudential supervisory responsibility
OCC	National banks (primary) Federal branches and agencies of foreign banks (primary) FSAs (primary)
Federal Reserve Board	Bank holding companies (primary) State member banks (primary) Savings and loan holding companies (primary) National banks (secondary) Federal branches and agencies of foreign banks (secondary)
FDIC	Insured state nonmember banks (primary) Insured state savings associations (primary) Insured national banks (secondary) Insured FSAs (secondary) Insured state member banks (secondary)

The Consumer Financial Protection Bureau examines and enforces certain federal consumer financial laws with respect to large insured depository institutions—those with more than $10 billion in total assets—and their holding companies and affiliates. For banks with total assets of more than $10 billion, the OCC evaluates the quantity of risk and the quality of compliance risk management through the OCC's Risk Assessment System and assigns consumer compliance ratings. For banks with total assets of $10 billion or less, the OCC is responsible for examining compliance with all applicable laws and regulations affecting consumers.

Bank boards also should be aware that certain activities may be subject to regulation by other federal and state agencies. For example, the U.S. Securities and Exchange Commission, the U.S. Commodity Futures Trading Commission, and state insurance commissioners are the primary regulators of bank subsidiaries engaged in securities, commodities, and insurance activities, respectively.[11]

[11] Banks also may have to register as swap dealers or security-based swap dealers with the Commodity Futures Trading Commission and the Securities and Exchange Commission, respectively. The OCC may examine any part of the bank, require reports related to any of its activities, and take other actions related to any of its activities—even those regulated by other agencies.

Board of Directors

Board's Role in Corporate and Risk 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 book 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 products and services or expand beyond current markets. 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.[12]

In most cases, nominees should be able to serve as directors immediately after they are elected in accordance with the bank's bylaws. When the bank is not complying with certain minimum capital requirements; is in a troubled condition, as defined by the regulation;[13] or is not complying with a directive to correct a problem promptly, the bank must file a prior notice with the OCC regarding proposed new directors before the proposed directors can be elected to the board.[14] The OCC also may object to proposed directors of new banks during the first two years of business.[15]

New directors should adhere to the attendance policy for regular and special board meetings. A director may not participate or vote by proxy.[16] 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 book.

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 ensure that directors 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.

---

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

[13] For more information, refer to 12 CFR 5.51(c)(7), "Definitions."

[14] 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." Also, refer to the "Changes in Directors and Senior Executive Officers" and the "Background Investigations" booklets of the *Comptroller's Licensing Manual*.

[15] For more information, refer to 12 CFR 5.20(g)(2), "Organizing Group."

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

These are the two most common structures for board leadership:

- The chair is independent of the chief executive officer (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 help ensure a more appropriate balance of power between the board and 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. Independent audit committees of large banks must have members with banking or related financial management expertise and must have access to their own independent counsel.[17] 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.

[17] For more information, refer to 12 CFR 363.5(b), "Committees of Large Institutions."

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.
- how 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. Individuals cannot 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 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 ensure that it receives 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 during stockholder derivative litigation.[18] 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.

---

[18] 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.

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.[19] 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.

Senior Management and Staff Access

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 managers promote.

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 Bank Secrecy Act (BSA)/anti-money laundering (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 those issues that pertain to their bank.

---

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

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.[20]

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 is responsible for setting and periodically reevaluating 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 capital minimums, the compensation paid to directors should be reassessed. This 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 ensure it has 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.

[20] 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, "Standards for Board of Directors"; and appendix D, III.E, "Provide Ongoing Training to All Directors."

Board's Responsibilities

The board is responsible for

- providing effective oversight.
- exercising independent judgment.
- providing credible challenge to management.
- holding management accountable for implementing policies and operating within established standards and limits.
- establishing an appropriate corporate culture and setting the tone at the top.
- complying with fiduciary duties and the law.
- understanding its role in monitoring the bank's operations.
- staying informed about the bank's operating and business environment.
- understanding the legal and regulatory framework applicable to the bank's activities.
- selecting and retaining a competent CEO and management team.
- overseeing the compensation and benefits programs.
- maintaining appropriate affiliate and holding company relationships.
- establishing and maintaining an appropriate board structure and performing board self-assessments.
- understanding the bank's material risks and confirming that the bank has a risk management system suitable for the bank's size and activities.
- setting realistic strategic goals and objectives and overseeing management's implementation of those goals and objectives.
- overseeing the bank's business performance and ensuring the bank serves community credit needs.
- ensuring the bank maintains an effective BSA/AML control structure.[21]

[21] For more information, refer to 12 CFR 21, "Minimum Security Devices and Procedures, Reports of Suspicious Activities, and Bank Secrecy Act Compliance Program," and the *Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

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.[22]

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 bank.[23]

When providing active oversight under paragraph III.B of these guidelines, each member of the board should exercise sound, independent judgment.[24]

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

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 maintain the bank's operations in a safe and sound manner, oversee compliance with laws and regulations, supervise major banking activities, and govern 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 reinforce and expand on supervisory expectations regarding the board's oversight duties and management's roles and responsibilities.

---

[22] For more information, refer to 12 CFR 30, appendix D, III, "Standards for Boards of Directors," and appendix D, III.A, "Require an Effective Risk Governance Framework."

[23] For more information, refer to 12 CFR 30, appendix D, III, "Standards for Boards of Directors," and appendix D, III.B, "Provide Active Oversight of Management."

[24] For more information, refer to 12 CFR 30, appendix D, III, "Standards for Boards of Directors," and appendix D, III.C, "Exercise Independent Judgment."

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

- set the expectations for desired behaviors, convey the expectations, and ensure those behaviors are linked to performance reviews and compensation practices.
- promote clear lines of authority and accountability.
- hold management accountable for the transparent and timely flow of information.

To promote a sound corporate culture, management should

- reinforce the corporate culture with all employees.
- integrate the culture into the bank's strategic planning process and risk management practices.
- ensure 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.

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.[25]
- **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 and directors must maintain the confidentiality of bank, customer, and personnel information.
- **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 board should ensure that there is a process for employees to report legitimate concerns about suspected illegal, unethical, or questionable practices with 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.

[25] 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*.

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.[26]

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), 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. 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.[27]
- misuses or misapplies bank funds or assets.[28]
- requests or accepts fees or gifts to influence, or as a reward for, bank business.[29]
- makes false statements generally.[30]
- commits or attempts to commit fraud.[31]
- willfully violates the BSA or its implementing regulations.[32]

---

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

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

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

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

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

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

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

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 ensure compliance 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 ensure that the CEO has the leadership skills and the appropriate competence, experience, and integrity to carry out his or her responsibilities.

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 ensure 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 the "Establish and Maintain an Appropriate Board Structure" section of this book.

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.[33]
- meet regularly with senior management and maintain appropriate lines of communication.

---

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

- ensure management provides the board with 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.

An FSA board must approve any employment contract that the association enters into.[34] The regulation 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.

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 ensures that the board discharges its responsibilities to supervise management and holds the CEO accountable. When the CEO does not fulfill board expectations, the board should be prepared to replace the CEO.

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

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

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 ensure that the plans remain viable.

The CEO is responsible for ensuring 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 the needs 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, chief audit executive (CAE), CRE, their direct reports, and other potential successors.[35]

Oversee Compensation and Benefits Arrangements

The board should determine that compensation practices for its executive officers and employees are safe and sound, are consistent with prudent compensation practices, and comply with laws and regulations governing compensation practices. For an FSA or its service corporation,[36] compensation to directors, officers, and employees must be reasonable and commensurate with their duties and responsibilities.[37] This requirement 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]

---

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

36 For more information regarding the applicability of this principle to mutual FSAs, refer to 12 CFR 5.59(e)(7), "Supervisory, Legal or Safety or Soundness Considerations."

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, "Interagency Guidelines Establishing Standards for Safety and Soundness," 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."

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 that ensure incentive compensation arrangements are consistent with regulatory guidance.
- evaluating executive performance relative to board-established goals and objectives.
- considering shareholder concerns.

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. The board and management should ensure that incentive compensation arrangements do not undermine the bank's safety and soundness by encouraging imprudent risk taking.

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. Incentive compensation arrangements should be supported by strong corporate governance, including active and effective oversight by the board. Smaller banks that are not significant users of incentive compensation should have programs tailored to the banks' size and complexity of operations.

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] OCC Bulletin 2010-24 applies 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. As outlined in OCC Bulletin 2010-24, incentive compensation arrangements should comply with the following principles:

- 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.

---

[40] The largest, most complex banks are defined in the "Large Bank Supervision" booklet of the *Comptroller's Handbook*.

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.
- 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 the "Establish and Maintain an Appropriate Board Structure" section of this book.

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 must meet 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 is responsible for all decisions relating to the cost and scope of the bank's employee benefits. The board also is 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.

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 parent 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. 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 ensure 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.

---

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.

42 For more information, refer to 12 USC 371c, "Banking 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 former *Office of Thrift Supervision (OTS) Examination Handbook.*

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, 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.[43] 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.

---

[43] 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.

The board's responsibility is to determine which committees it needs to effectively govern the bank. The committees vary by bank. The following pages describe some key committees. This list is not exhaustive or a required list of committees, unless they are mandated by laws or regulations.

Executive Committee

Some boards choose to use an executive committee. When utilized, the board traditionally authorizes the executive committee to act on the board's behalf. The executive committee usually addresses matters requiring board review that arise between full board meetings. The executive committee can relieve the full board of detailed reviews of information and operational activities. The executive committee may also coordinate the work of other board committees. The executive committee, however, should not have 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 ensure that the charter clearly specifies the committee's authority and what the committee may approve on the board's behalf.

The board should ensure that the use of the executive committee does not lead to a two-tiered class of directors in which the executive committee wields all the power. All directors have the same responsibilities and liabilities. The executive committee should not be viewed as a seat of power or as the most prestigious committee.

The executive committee should not be confused with executive sessions of the independent directors of the board.

Audit Committee

The audit committee, or its equivalent, should oversee the bank's audit program to ensure it is sufficiently robust to identify, test, and report on all key risks in the bank. All banks should have an audit committee. The bank's size dictates the composition of the audit committee.

The main areas of responsibility of the audit committee are as follows.[44] The list summarizes sound practices for the bank's audit committee.

- Work with internal and external auditors to ensure that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities.
- Ensure that senior management establishes and maintains an adequate and effective internal control system and processes.
- Hold committee meetings with a frequency that facilitates oversight, that is, at least four times a year.

---

[44] For more information on audit committee requirements and responsibilities for national banks, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*. For FSAs, refer to sections 350, "External Audit," and 355, "Internal Audit," of the former *OTS Examination Handbook*. Also refer to the Basel Committee on Bank Supervision, "The Internal Audit Function in Banks," June 2012. Annex 2 provides an overview of the responsibilities of an audit committee.

- Establish schedules and agendas for regular meetings with internal auditors, along with external auditors when providing oversight.
- Carry out the appointment and termination, setting of compensation, and assessment of performance of the CAE or equivalent and the independent public accountant or external auditor.[45]
- Ensure external auditors are independent and objective in their findings and consistent with their independence principles and rules. Ensure that external auditor engagement letters and any related agreements for services do not contain any unsafe or unsound limitation of liability provisions before the engagement.[46]
- Monitor the financial reporting process and oversee the bank's establishment of accounting policies and practices. Review the significant qualitative aspects of the bank's accounting practices, including accounting estimates, financial reporting judgments, and financial statement disclosures.
- Establish and maintain procedures (also known as whistle-blower procedures) for bank employees to submit confidential and anonymous concerns to the committee about questionable accounting, internal accounting control, or auditing matters.[47] Procedures should be set up for timely investigation of complaints received and appropriate documentation retention.
- Meet with bank examiners at least once each supervisory cycle to discuss findings of OCC reviews, including conclusions regarding audit.
- Monitor, track, and hold management accountable for addressing deficiencies that auditors or regulators identify. Also, when necessary, provide discipline to ensure effective and timely response by management to correct control weaknesses and violations of law or regulation noted in internal or external audit reports or in examination reports.

---

[45] According to 12 CFR 363.4, "Filing and Notice Requirements," notification to regulators must be made on the termination of the external auditor. Also refer to 12 CFR 363.5(c), "Independent Public Accountant Engagement Letters."

[46] The board and any audit committee of all banks have this responsibility. For banks subject to 12 CFR 363, "Annual Independent Audits and Reporting Requirements," however, these unsafe and unsound provisions include those that indemnify the independent public accountant against claims made by third parties; hold harmless or release the independent public accountant from liability for claims or potential claims that might be asserted by the client bank, other than claims for punitive damages; or limit the remedies available to the client bank.

[47] According to OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing," when the board fulfills the audit committee responsibilities, the procedures should provide for the submission of employee concerns to an outside director, timely investigation of complaints received, and appropriate documentation retention.

Heightened Standards

The audit committee reviews and approves internal audit's overall charter and audit plans. The audit committee should also approve all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The committee may also oversee the CAE's administrative activities or designate them to the CEO.[48]

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.[49]

Credit Committee

The credit committee oversees management's handling of credit risk to ensure compliance with board decisions regarding the bank's lending strategy and credit risk appetite and limits. The committee should review and approve the bank's lending policies and monitor the lending officers' compliance with such policies. The credit committee should verify that management

- recognizes adverse trends.
- enables early detection of problems in the loan portfolio.
- takes timely and appropriate sustainable corrective actions.
- maintains an adequate allowance for loan and lease losses (ALLL).

The credit committee should oversee the bank's credit risk management practices to ensure they safeguard against noncompliance with loan-related laws and regulations and the bank's lending policies. In many banks, this committee also approves loan applications for credits involving large dollar amounts relative to the banks' size and capital levels. The bank's loan review function should periodically report to the credit committee its conclusions on the effectiveness of the loan rating systems and credit risk management practices. In addition, the credit committee should monitor loan policy exceptions and review (and approve) changes or additions to the bank's underwriting standards.

Asset-Liability Committee

In most banks, the board delegates responsibility for establishing specific interest rate risk, liquidity, and other asset-liability strategies and oversight to a committee of senior managers. If there is a board-level asset-liability committee, the committee should

- establish and guide the bank's strategy as well as liquidity and interest rate risk appetite.

---

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

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

- identify senior managers who have authority and responsibility for managing these risks.
- monitor the bank's performance and overall interest rate risk profile and liquidity position, ensuring that asset-liability strategies are prudent and are supported by adequate capital and liquidity.
- ensure the bank implements sound risk management practices to identify, measure, monitor, and control interest rate and liquidity risks.
- verify that adequate resources are devoted to asset-liability management.

Regulations require the board of an FSA to monitor financial derivatives activities and interest rate risk. The board must adopt appropriate policies and procedures and periodically review them.[50] While the regulations apply only to FSAs, the guidelines contain sound practices that all banks should follow.

Risk Committee

The risk committee's primary responsibility is risk oversight. For smaller banks, the audit committee sometimes assumes the oversight of risk management activities. Banks that have increased complexity customarily establish a separate risk committee. While not required, larger banks often have a bank 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 to ensure 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 strategic plan.
- reviewing and approving risk limits.
- ensuring 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.
- regularly discussing the bank's material risks in aggregate and by risk type.
- regularly discussing the effect of the risks to capital, earnings, and liquidity under normal and stressed conditions.
- ensuring the independence of the risk management functions.
- overseeing and directing the work of the CRE or equivalents.
- ensuring effective and timely escalation of material issues to the board and holding management accountable for timely and appropriate corrective action.

---

50 For more information, refer to 12 CFR 163.172, "Financial Derivatives," and 12 CFR 163.176, "Interest-Rate-Risk-Management Procedures."

Heightened Standards

The board or its risk committee should approve the risk governance framework and any significant changes.[51] The board or its risk committee also should monitor compliance with the risk governance framework.[52] Each CRE should have unrestricted access to the board risk committee regarding risk and issues identified through IRM activities.[53] The board or its risk committee approves the appointment and removal of a CRE and the CRE's annual compensation and salary adjustment.[54] The board or its risk committee demonstrates support for IRM by ensuring that IRM has the resources needed to carry out its responsibilities and by relying on IRM's work when carrying out its oversight responsibilities.[55] The risk committee is generally a stand-alone committee, distinct from the audit committee.[56]

Fiduciary Committee

A bank with fiduciary (trust) powers has a number of fiduciary responsibilities that include ensuring compliance with both state and federal laws and regulations governing fiduciary activities.[57] To ensure compliance and appropriate oversight of fiduciary activities and asset management products and services, the board typically establishes three fiduciary committees: one for administrative decisions, one relating to investment oversight, and a fiduciary audit committee. 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.[58] 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.

---

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

[52] Ibid.

[53] For more information, refer to 12 CFR 30, appendix D, I.E.7, "Independent Risk Management."

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] For more information on a national bank's fiduciary responsibilities and compliance with 12 CFR 9, "Fiduciary Activities of National Banks," refer to the "Asset Management" and "Internal and External Audits" booklets of the *Comptroller's Handbook*. For information on FSAs, refer to 12 CFR 150, "Fiduciary Powers of Federal Savings Associations"; to sections 350, "External Audit," and 355, "Internal Audit," of the former *OTS Examination Handbook;* and to the "Asset Management" booklet of the *Comptroller's Handbook*.

[58] For more information, refer to 12 CFR 9.9, "Audit of Fiduciary Activities."

Compensation Committee

A bank may have a compensation committee to oversee compensation arrangements. This oversight includes the design and implementation of any incentive compensation arrangements for covered employees as discussed in the "Oversee Compensation and Benefits Arrangements" section of this book. The committee may also review and recommend compensation for directors, including the board and board committee fee structure. The committee should provide periodic reports to the full board on compensation and benefits matters. The committee should work closely with board-level risk and audit committees to ensure that all committee decisions align with the bank's strategic objectives and risk appetite, and appropriately balance risk and reward. In fulfilling its responsibilities, the committee should have an understanding of all the bank's compensation and benefits arrangements, including

- the use of performance measures that are based solely on industry peer performance comparisons.
- the relationship between the bank's compensation arrangements and the risks or behaviors that the arrangements may incentivize.
- whether compensation arrangements are designed to promote long-term shareholder value and not promote excessive risk taking.
- the legal requirements governing executive compensation arrangements.

The compensation committee may assume other responsibilities, such as overseeing the bank's employee benefits plans. If the committee oversees these activities, it should ensure 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. In doing so, the committee should determine that no more than reasonable compensation is paid to the third party out of employee benefit plan assets.

Corporate Governance/Nominating Committee

At many banks, the corporate governance/nominating committee duties involve

- recommending nominees for election to the board.
- 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.

As part of its director nomination process, the corporate governance/nominating committee should establish criteria for board and committee membership, including qualifications and independence requirements. This committee may evaluate new nominees' qualifications. The committee may also assess the contributions of current directors in connection with their re-nomination. The committee can help ensure 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.[59]

Other responsibilities of the corporate governance/nominating committee 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.

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 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.

---

[59] For more information, refer to 12 CFR 5.21(j)(2), "Bylaws for Federal Mutual Savings Associations."

A board self-assessment addresses the effectiveness of the board's structure, activities, and oversight, 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.[60]

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.[61] The reports should be accurate, timely, relevant, complete, and succinct. Refer to the "Maintain Management Information Systems" section in this book for more information about management information systems (MIS). The information requirements, particularly the number and variety of reports, depend on the bank's size, complexity, and risks. The board and management should ensure that the information is sufficient to keep relevant parties informed of the financial condition and performance of all the bank's material lines of business. In addition, the board and management should make sure that

---

[60] For more information, refer to 12 CFR 30, appendix D, III, "Standards for Board of Directors."

[61] 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*.

information requirements 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 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 loss analysis
- Concentrations of credit
- Liquidity position and trends and contingency funding plans
- Interest rate sensitivity analyses
- Performance metrics for new 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 vis a vis risk appetite, performance goals, and strategic goals
- Earnings trends and quality, including non-interest income and expenses

Serve the Community Credit Needs

Each bank has a responsibility to help meet the credit needs of its communities, consistent with safe and sound lending practices, and has an obligation to ensure fair access and equal treatment to all bank customers. The CRA is intended to prevent redlining and to encourage banks to help meet the credit needs of all segments of their communities, including low- and moderate-income neighborhoods.[62]

The board 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 ensure 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 likely a function of the bank's size and complexity as well as the committee work required of the director.

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.

---

[62] 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 former *OTS Examination Handbook*.

Request and Review Meeting Materials

The board is responsible for working with management to determine what information the board needs at meetings to monitor the bank's operations, make decisions, and ensure 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 ensure 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 book 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 ensure 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.[63] Refer to the "Establish an Appropriate Corporate Culture" section in this book for more information.

---

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

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[64] of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank.[65]
- should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the OCC's satisfaction.[66]

Board and Management's Roles in Planning

The board is responsible for establishing the bank's goals and for overseeing that the bank has the personnel as well as the financial, technological, and organizational capabilities to achieve those goals. Ongoing changes in the banking industry make it essential for the bank to 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

---

[64] As defined in 12 CFR 225.41(b)(3), "Immediate Family," of Regulation Y.

[65] As defined in 12 CFR 215.2(e)(1), "Executive Officer," of Regulation O.

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

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 must 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 the board and management to measure the actual and potential risks associated with achieving the bank's strategic goals and objectives. 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, 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 and developing policies and processes to guide the plan's execution. Management also should develop monitoring systems to report actual outcomes, report key performance indicators and key risk indicators, and ensure that the bank's objectives and risks remain aligned with the risk appetite.

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.[67]

New Products and Services

A key consideration in the bank's strategic planning process is growth and new profit opportunities for the bank. These opportunities include expanding

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

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 products and services often require substantial systems support, new expertise, substantial lead time, and significant financial investment. Planning for these new activities should include assessing potential risks and returns and establishing performance objectives that are carefully monitored as new products and services are initiated.[68] Management should ensure that the board or delegated committee has reviewed and approved plans for new activities and that the plans clearly articulate the potential risks and returns.

Policies should be in place before the bank engages in any new activity. The board and management should oversee all new, expanded, or modified products and services through an effective risk management process. The risk management process should include

- performing adequate due diligence before introducing a product or service.
- developing and implementing controls and processes to ensure risks are properly measured, monitored, and controlled.
- developing and implementing appropriate performance monitoring and review systems.

The formality of the bank's risk management process should reflect the bank's size and the complexity of the product or service offered. Depending on these factors, it may be appropriate for the bank to establish a senior management or risk committee to oversee development and implementation of the product or service.

Capital Planning

Capital planning is integral to ensuring safe and sound operations and viability. The board and senior management should ensure that the bank has sufficient capital that fully supports the current and anticipated needs of the bank. 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 to ensure capital adequacy.[69] The capital planning process and the resulting capital plan need to evolve as the bank's overall risks, activities, and risk management practices change. The most effective capital

---

[68] For more information regarding national banks, refer to OCC Bulletin 2004-20, "Risk Management of New, Expanded, or Modified Products and Services: Risk Management Process." For more information regarding FSAs, refer to section 760, "New Activities and Services," of the former *OTS Examination Handbook*.

[69] For more information, refer to OCC Bulletin 2012-16, "Capital Planning: Guidance for Evaluating Capital Planning and Adequacy."

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.

Capital planning is especially critical for mutual FSAs, which are subject to the same regulatory capital requirements as stock banks.[70] Unlike stock banks, mutual FSAs have very limited means to increase regulatory capital quickly and build capital almost exclusively through retained earnings.

Stress testing is an essential 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. Effective stress testing enables the board to consider the impacts to capital under various scenarios (for example, best, most likely, and worst case). The results of the stress testing may help management develop action plans to address negative outcomes. For community banks with total assets up to $10 billion, the sophistication and rigor of stress testing depends on the bank's size, portfolio risk, and complexity.[71]

For banks with total assets greater than $10 billion, Dodd–Frank requires annual stress testing.[72] The board and management should establish a comprehensive, integrated, and effective stress-testing process that fits into the bank's broader risk management.

As part of the board's oversight of capital planning, it should direct management to ensure the integrity, objectivity, and consistency of the capital planning process. The board should review and approve its capital planning process and capital goals at least annually, or more frequently as warranted. The board should ensure that the planning process addresses the bank's capital needs in relation to material risks and strategic plans. In addition, the board and management should evaluate internal and external sources of capital to develop a strategy to increase capital whenever necessary. An effective board holds management accountable for identifying and taking sustainable corrective actions if shortcomings or weaknesses in the capital planning process become apparent or if the level of capital falls below identified needs.

Senior management is responsible for developing a capital plan that integrates the bank's strategy, risk management, and capital and liquidity planning decisions. The capital planning process should include

---

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

[71] For more information, refer to OCC Bulletin 2012-33, "Community Bank Stress Testing: Supervisory Guidance."

[72] For more information, refer to 12 CFR 46, "Annual Stress Test"; OCC Bulletin 2012-14, "Interagency Stress Testing Guidance"; and OCC Bulletin 2014-5, "Dodd–Frank Stress Testing: Supervisory Guidance for Banking Organizations With Total Consolidated Assets of More Than $10 Billion but Less Than $50 Billion."

- identifying and evaluating risks.
- setting and assessing capital adequacy goals that relate to risk.
- maintaining a strategy to ensure capital adequacy and contingency planning.
- ensuring integrity in the internal capital planning process and capital adequacy assessments.

Senior management should anticipate changes in the bank's strategic direction, risk profile and risk appetite, business plans, operating environment, and other factors that materially affect capital adequacy. Senior management should establish contingency plans, including identification or enhancement of realistic strategies for capital preservation during economic downturns or other times of stress.

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,[73] 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.[74]

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.

---

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

[74] For more information, refer to the "Business Continuity Planning" booklet of the *FFIEC Information Technology (IT) Examination Handbook*.

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

Information Technology Activities

Banks rely heavily on IT to process bank transactions, maintain critical records, and supply reports to the board and management about managing business risk.[75] 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. Board and management responsibilities include third-party relationship risk management and safeguarding customers' nonpublic information.

The board should demonstrate that it has an adequate understanding of the bank's IT infrastructure, inherent risks, and existing 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.

Information Security

Banks are critically dependent on their information and technology assets, such as hardware, software, and data. The board and management should protect information and technology assets to ensure 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,

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

confidentiality, and integrity of customer information.[76] The guidelines also discuss assigning specific responsibility for implementing an information security program and reviewing reports from management.

Based on the guidelines, the board is responsible for overseeing the 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.

Board and Management's Roles in 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.

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. The interrelationship of the bank's risks and the potential impact on its earnings, capital, and strategic objectives require the risks to 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 from a single business line or multiple business lines that, when aggregated, represent concentration risk that may require board 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 from a corporate standpoint.

---

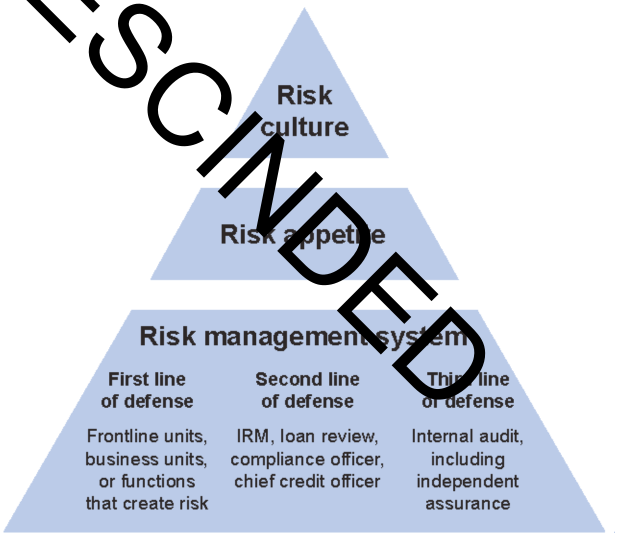
[76] For more information, refer to 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards."

Risk Governance Framework

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

- 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.

The board is responsible for overseeing the design and implementation of the risk governance framework. The board should require periodic independent assessments to determine the framework's effectiveness, which may involve reviewing components of or all of the framework.

Senior management is responsible for developing and maintaining the risk governance framework, 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.

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.[77] 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.[78] 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.[79] 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 the risk profiles of the parent company and covered bank are substantially the same.[80]

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 ensuring the bank operates 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 ensure material risks and risk-taking activities exceeding the risk appetite are recognized, escalated, and addressed 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.

---

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

[78] Ibid.

[79] Ibid.

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

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 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).[81]
- establish appropriate metrics for measuring and monitoring risk results.
- ensure 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 an escalation process to ensure that material weaknesses or problems are escalated to senior management (without fear of retribution), the CRE, and the risk committee or designated committee, as appropriate.

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

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.[82] To be effective, the bank's risk appetite statement must be communicated and implemented throughout the bank.[83]

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.[84]

The risk appetite statement should be communicated to all employees to ensure that their risk-taking decisions align with the 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.[85]

Risk Management System

The bank's risk management system comprises its policies, processes, personnel, and control systems, which are further discussed in the "Administer a Risk Management System" section of this book. 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 proportionate to the risks present and the size and complexity of the bank.

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; and (3) internal audit.

---

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

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

[84] Ibid.

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

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 chief 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.

The board should oversee the bank's risk management system to ensure 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.

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

- keep directors adequately informed about risk-taking activities.
- implement the bank's or holding company's strategy.
- develop policies that define the bank's risk appetite and ensure they 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 MIS to ensure the information is timely, accurate, and relevant.

Heightened Standards

The risk governance framework should include well-defined risk management roles and responsibilities for frontline units, IRM, and internal audit.[86] Frontline units should assess, on an ongoing basis, the material risks associated with their activities.[87] 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.[88]

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.[89]

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.[90]

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.[91]

The board is responsible for ensuring that a system of internal controls is in place. The board should periodically receive information about the effectiveness of the bank's internal controls and information systems.

---

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

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

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

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

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

[91] 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 former *OTS Examination Handbook*.

Senior management should design and implement a system of internal controls that readily identifies, measures, monitors, and controls risk. 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.

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 helps the board and management address emerging risks at an early stage and allows them to develop and implement 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 also 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.

Compliance Management Program

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.[92] Compliance management programs should extend beyond consumer protection laws and factor in all applicable laws and regulations, as well as prudent ethical standards

---

[92] 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."

and contractual obligations. Therefore, the board and management should recognize the scope and implications of laws and regulations that apply to the bank and its activities. It is important for the board and management to understand the potential consequences of violations of laws and regulations that may result in CMPs, financial losses, reputation and legal risks, and enforcement actions.

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.

Management should implement an effective risk management system and internal controls to ensure compliance with all applicable laws and regulations. To reinforce the board's position on compliance, management should clearly communicate an expectation that compliance with all laws and regulations is an organizational priority for all employees. For more information on management's responsibilities, refer to the "Compliance Management" section of this book.

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.[93] The audit program consists of an internal audit function and an external audit. 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 audit should be independent of the audited activities with sufficient stature, authority, and board support to carry out its assignments with objectivity. Similarly, the external auditor provides assurances of the system of internal controls over the bank's financial statements. When a third-party service provider provides both audit and consulting services, special care should be taken to ensure that the firm does not audit the activities for which it provided consultation services.[94]

The board should not delegate internal audit oversight responsibilities to management. The board may, however, 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.

Board responsibilities for overseeing the internal and external audit functions are generally delegated to an audit committee, which is discussed in the "Establish and Maintain an Appropriate Board Structure" section of this book. Ultimately, the board is responsible for staying apprised of

---

[93] For more information on the OCC's expectations for effective audit functions, for national banks refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*. For FSAs, refer to sections 350, "External Audit," and 355, "Internal Audit," of the former *OTS Examination Handbook*.

[94] 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."

material audit findings and recommendations and for holding management accountable for taking sustainable corrective actions to address issues identified by auditors or regulators.

When the internal audit function is performed in-house, the CAE or chief auditor, if applicable, leads the function. The chief auditor reports directly to the audit committee. Administratively, the chief auditor may report to the CEO. The chief auditor is responsible for implementing the audit program and reporting 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. When the bank outsources the internal audit function, the board and senior management should designate an audit liaison to coordinate audit activities.

Accountability to Shareholders and Other Stakeholders' Accountability

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 enhances the bank's value and potentially provides access to capital and funding markets.

Management's Responsibilities

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. The board delegates authority to senior management for directing and overseeing day-to-day management of the bank. Senior management is responsible for developing and implementing policies, procedures, and practices 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 is responsible for carrying out the bank's day-to-day activities and financial performance. Management should ensure it optimizes earnings from 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 are responsible for

- executing the bank's strategic plan and ensuring the adequacy of capital and resources in carrying out the strategic plan.
- developing a risk management framework that enables management to effectively identify, measure, monitor, control, and report on risk exposures consistent with the bank's risk appetite.
- implementing a strong risk culture and ethical standard and providing incentives to reward appropriate behavior.
- establishing and maintaining an effective system of internal controls.
- developing accurate and reliable management information and reporting systems.
- maintaining internal processes, including stress testing when appropriate, to ensure capital and liquidity levels are commensurate with the bank's risks in normal and stressed conditions.
- ensuring the appropriate allocation of staff resources and effectively overseeing personnel.
- complying with laws, regulations, and internal policies, including ethics policies and policies governing insider activities.
- establishing talent management and compensation programs.
- keeping the board apprised of the bank's strategic direction, risk profile, risk appetite, business operations, financial performance, and reputation.

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 committees include asset-liability committee, credit, compliance, and IT steering.

The following pages focus on some of the key responsibilities of the CEO and senior management.[95]

Administer a Risk Management System

Management is responsible for the design, implementation, and ongoing monitoring of the bank's risk management system. The risk management system should reflect the bank's risk profile, size, and complexity. As the bank grows, systems should keep pace and evolve in sophistication.

While risks historically were concentrated in traditional banking products and services, community banks now offer a wide array of new and complex products and services. Therefore, risk management systems in community banks vary in accordance with the banks' complexity and volume of risk. The risks that large and midsize banks assume are varied and complex, due to the banks' diversified business lines and geographies. Because of increased complexity and risks, risk management systems in larger, more complex

---

[95] For more information on specific management responsibilities and risk management processes for business lines and their risks, refer to various booklets in the *Comptroller's Handbook*, including "Community Bank Supervision," "Large Bank Supervision," and "Federal Branches and Agencies Supervision."

banks should be sufficiently comprehensive to enable senior management to identify and manage the risk throughout the company.

Regardless of the bank's size and complexity, a sound risk management system should do the following:[96]

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, the board and management also should identify 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 ensure that risks are appropriately addressed. Risk identification in merging companies begins with establishing uniform definitions of risk; a common language helps to ensure 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 ensure 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, the resulting company should make a concerted effort to ensure 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 ensure timely review of risk positions and exceptions. 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 ensure 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 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

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

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.

Management's responsibilities for the implementation, integrity, and maintenance of the risk management system should include the following:

- Keep directors adequately informed about risk-taking activities and outcomes.
- Implement the bank's strategy.
- Develop policies that define the bank's risk appetite and ensure the policies are compatible with strategic goals.
- Ensure that the strategic direction and risk appetite are effectively communicated and adhered to throughout the bank.
- Oversee the development and maintenance of MIS to ensure that information is timely, accurate, and relevant.

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, so is the bank's risk management.

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 designate board committee is responsible for approving designated policies, management is responsible for developing and implementing the policies. The CEO and management should ensure that policies are periodically reviewed 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 where senior management relies on a widely dispersed staff to implement complex business strategies. In addition, management should ensure that appropriate policies are in place before engaging in any new activities.

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 determines 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, compliance management system, and compensation program, which are discussed throughout this book. Refer to 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[97] 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 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 increases, 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 ensuring that staffing is commensurate with the bank's risk profile.

---

[97] 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 former *OTS Examination Handbook*.

The board and management should design programs to attract, develop, and retain qualified personnel. An effective recruitment program enhances the continuity of executive and middle management, and ensures 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 community banks with limited staff, depth, and overlap of responsibilities, training and development is vital to ensure smooth, 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 to ensure the appropriate depth and breadth of staff.

Management should create and maintain an organizational structure that ensures clear lines of responsibility, accountability, and oversight. Management should ensure that personnel in risk management and audit 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 ensures 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.

Ensure Control Functions Are Effective

Quality Control

Quality control ensures 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 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 ensure that results of the reviews are reported to appropriate personnel.

Compliance Management

The CEO and management must ensure the bank complies with applicable laws and regulations, and should ensure that the bank complies with board-approved policies, prudent ethical standards, and contractual arrangements. Management should develop a system to monitor compliance, including the training of appropriate personnel, and ensure timely correction of any fraud or violations that are detected. The compliance management system should consist of a compliance program and a compliance audit function.[98] The compliance program includes the policies, procedures, and processes as well as the monitoring and testing programs that ensure personnel adhere to applicable laws and regulations and board-approved policies. The compliance audit function allows the board and management to monitor the effectiveness of its compliance management system and assists in the detection of fraud or violations of laws and regulations. The CEO and management are responsible for the timely correction of deficiencies found by internal and external auditors, compliance personnel, risk managers, and regulators. The CEO and management also are responsible for ensuring that processes promptly escalate material issues to the board and senior management. Management also should ensure there is a mechanism for employees to confidentially raise concerns about illegal activities and violations. The mechanism also should allow employees to confidentially report circumvention of regulations or company policies.

---

[98] For more information, refer to the "Compliance Management System" booklet of the *Comptroller's Handbook*.

Many banks establish a separate compliance function headed by a compliance officer or committee. The bank's compliance program may focus on a number of areas, including consumer protection, regulatory compliance with lending and investment activities, bank operations, securities issues, tax law, and insider activities. Compliance officers should ensure appropriate training for all bank employees on relevant compliance issues. Compliance officers should ensure the bank has established adequate monitoring and testing programs. Compliance officers also should have a process to identify the applicable laws and regulations and stay abreast of evolving regulatory requirements. Management should establish metrics to monitor performance. Management also should ensure compliance-related roles and responsibilities are clearly established and communicated.

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.[99] The board is responsible for approving the BSA/AML compliance program and for overseeing the structure and management of the organization's BSA/AML compliance function.[100] The program must include

- a system of internal controls to ensure ongoing compliance.
- independent testing for compliance.
- a designated individual responsible for coordinating and monitoring day-to-day compliance.
- training for appropriate personnel.
- appropriate risk-based procedures for conducting ongoing customer due diligence, including, but not be limited to
  - understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
  - conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[101]
- a customer identification program.[102]

Maintain Management Information Systems

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 must 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.

---

99 For more information, refer to the *FFIEC BSA/AML Examination Manual*.

100 For more information, refer to 12 CFR 21, subpart C, "Procedures for Monitoring Bank Secrecy Act Compliance."

101 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."

102 For more information, refer to 12 CFR 21.21(2), "Customer Identification Program."

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 promptly.

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 comprehensive internal and external audit program to ensure 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 supports 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.[103]
- The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.[104]

Manage Third-Party Relationship Risks

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 risk management processes commensurate with the level of risk and complexity of the bank's third-party relationships and organizational structure.[105] 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. During supervision of the process, management should ensure appropriate oversight and accountability, documentation and reporting, and independent reviews.

Ensure an Appropriate Insurance Program

Part of management's responsibility is to ensure a sound insurance program that identifies risk to be retained versus risk to be transferred. Management can implement additional controls to minimize and retain risk. Management

---

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

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

[105] For more information, refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," and the "Outsourcing Technology Services" booklet of the *FFIEC IT Examination Handbook*.

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. The board and 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 program annually.

The following pages explain major types of insurance coverage available to banks. The names of the insurance coverage may differ among banks.

Indemnification Agreements

A bank director may not be able to avoid being 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.

Regulation limits indemnification agreements.[106] For administrative proceedings or civil actions initiated by a federal banking agency, 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).[107] Payment of liability or legal expenses is prohibited for 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.[108]

---

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

[107] Refer to 12 USC 1813(u), "Institution-Affiliated Party," for the full definition.

[108] For more information, refer to 12 CFR 359.1(l), "Prohibited Indemnification Payment."

An exception permits reasonable indemnification payments if the IAP was exonerated. Reasonable indemnification payments are permitted[109] subject to the board making specific determinations and following specific procedures.[110] When reasonable indemnification payments are permitted, FSAs—but not national banks—are required to obtain OCC non-objection before making any indemnification payments.[111]

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 (1) the expense of defending suits alleging director or officer misconduct, and (2) 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

---

109 For national banks, refer to 12 CFR 7.2014, "Indemnification of Institution-Affiliated Parties."

110 For more information, refer to 12 CFR 359.5, "Permissible Indemnification Payments."

111 For more information regarding FSAs, refer to 12 CFR 145.121, "Indemnification of Directors, Officers and Employees."

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 book 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; ensure 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.[112]

Specialized Bank Insurance

The board and management may decide that they should obtain other bank insurance coverage to transfer risks. The following are some of the most frequently purchased 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)

---

112 For more information, refer to OCC Bulletin 2004-56, "Bank-Owned Life Insurance: Interagency Statement on the Purchase and Risk Management of Life Insurance."

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 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.

Supervision of Problem Banks

When the OCC identifies or communicates problems or weaknesses to a bank, the OCC expects the bank's senior management and board to take corrective action promptly. The steps the bank takes or agrees to take in response to problems or weaknesses are important factors in determining whether the OCC takes enforcement action and the severity of that action. If the OCC believes a bank has significant weaknesses, the OCC may conclude that the bank requires additional or special supervision. In such cases, the OCC examines and monitors the bank more frequently. The OCC works with the board and bank management to determine necessary corrective action to return the bank to a safe and sound condition.

Problem banks generally have composite CAMELS ratings of 3, 4, or 5 and often possess one or more of the following deficiencies:

- Excessive growth or inappropriate, aggressive growth strategies.
- Ineffective, dominant, or dishonest management, or material vacancies in management positions.
- Insider or affiliate transaction abuse and fraud.
- Excessive amount of low-quality assets.
- Inordinate concentrations of credit or investments.
- Insufficient capital.
- Inadequate policies, procedures, or internal controls.
- Deferred loan loss provisions, charge-offs, or recognition of securities impairment.
- Strained liquidity, including reliance on brokered deposits.
- Significant medium- and long-term interest rate risk exposure.
- Lack of a viable strategic plan.
- Failure of the board or senior management to understand the bank's activities and their risks.

A problem bank becomes subject to a number of enhanced regulatory restrictions as its composite or component CAMELS ratings or prompt corrective action (PCA) capital category declines or when it is subject to a formal enforcement action. The board is responsible for oversight of bank management's compliance with these restrictions.

Administrative Actions

Because the OCC and a bank's directors and management have a mutual interest in improving the condition of a bank in which the OCC has identified problems, it is beneficial to both parties to take corrective action promptly. The OCC decides on a case-by-case basis whether to bring an action against a bank, a director, or another IAP and the nature and extent of the action. The OCC considers how best to correct violations and unsafe or unsound banking practices and to prevent future bank problems. Key factors in the OCC's decision-making process include

- the seriousness of the problems or the violations of law.
- the board's history of cooperation with the OCC.
- the apparent ability and willingness of the board to take the appropriate corrective actions.

The examination exit meeting with bank management may be the bank's first indication that the OCC has concerns about the bank and is considering an administrative action. Directors may attend this meeting and should use this opportunity to seek advice about how to correct existing or potential problems.

Directors also may request a meeting with other OCC personnel (such as supervisory office and legal staff) if the OCC has indicated that it is considering an administrative action. OCC personnel would discuss the reasons for the proposed action as well as the specific problems the board should address.

The period between the end of an examination and the time when the examiners formalize the findings in a report of examination provides a good opportunity for the bank to formulate, finalize, and begin to carry out a reasonable plan to correct problems that examiners noted. The board should document in the board minutes the actions that it proposes to deal with these concerns. In addition, the OCC encourages, and under certain circumstances requires, banks to submit responses stating their commitment to a corrective actions plan and specifying the terms of the plan. During this period, the bank is encouraged to stay in contact with its OCC supervisory office and to work with the OCC to respond promptly and positively to the agency's concerns.

Good-faith discussions between the board and the OCC generally are successful in bringing about a speedy and mutually acceptable resolution of differences. These discussions should focus on devising a realistic and reasonable method to restore the bank to a safe and sound condition. A problem bank's failure to correct cited problems promptly and decisively will result in more severe OCC action.

Actions Against Banks

This section outlines the types of remedies available to the OCC to address problems in a bank. These remedies are designed primarily to direct the board and management to take appropriate corrective action to resolve deficiencies in bank operations.

The OCC may choose to take actions to correct specific problems identified at a bank. Actions typically specify what the bank needs to do to correct identified problems, such as improving lending practices, raising capital, instituting proper policies and procedures, or correcting specific violations of law. These actions may take the form of an informal or formal enforcement action. All formal enforcement actions are public documents; informal enforcement actions are not. The OCC also may assess a CMP against a bank or, under certain situations, appoint a receiver or conservator for the bank.

The OCC may take an enforcement action against a bank after obtaining the consent of the bank's board about the remedies to correct problems. If the OCC does not receive such consent, it may begin an administrative proceeding to impose a formal enforcement action. The OCC also has the authority under PCA to impose certain requirements on a bank in the absence of consent and without the normal administrative process. (Refer to "Formal Enforcement Actions" later in this section for a discussion of PCA.) Whether the administrative action is entered into by consent or imposed through an administrative proceeding, all directors are responsible for the bank's compliance with the action. While the enforcement action remains outstanding, the OCC will assess the bank's compliance with the enforcement document at least every six months. Enforcement actions, with the exception of temporary C&D orders, remain in effect until the OCC determines that the bank's overall condition has improved significantly, and the bank has achieved sustained compliance with the terms of the document. After the OCC has made this determination, the OCC may terminate the enforcement action.

Informal Enforcement Actions

Commitment Letter

A commitment letter is a document signed by the bank's board on behalf of the bank and acknowledged by an authorized OCC official, reflecting specific written commitments to take corrective actions in response to MRAs. Either the OCC or the bank may draft the document. A commitment letter is not a binding legal document. Failure to honor the commitments, however, provides strong evidence of the need for formal action.

Memorandum of Understanding

A memorandum of understanding (MOU) is a bilateral document signed by the bank's board on behalf of the bank and an authorized OCC representative. The OCC drafts an MOU, which in form and content looks very much like a formal OCC enforcement document. An MOU legally has the same force and effect as a commitment letter.

Safety and Soundness Plan

The OCC issues to the bank a determination and notification of failure to meet safety and soundness standards (collectively called a notice of deficiency) and requires the submission of a safety and soundness compliance plan.[113] At a minimum, the plan must include a description of the steps the bank will take to correct the deficiencies and the time within which the bank plans to take these steps. If the OCC approves the safety and soundness plan, the plan functions as an informal enforcement action. If the bank fails to submit an acceptable safety and soundness plan, however, or fails in any material respect to implement an approved plan, the OCC must, by order, require the bank to correct the deficiencies (refer to "Safety and Soundness Order" in the "Formal Enforcement Actions" section of this book). The OCC, by order, may require the bank to take any other action that the OCC determines would better carry out the standards for safety and soundness.

Individual Minimum Capital Ratio

A regulation establishes minimum capital requirements for all banks.[114] When appropriate, the OCC may establish higher capital requirements for a particular bank. Unless there are immediate time constraints, the OCC gives a bank notice and opportunity to comment on a proposal to increase the bank's minimum capital requirement.

One manner in which the OCC increases a bank's capital requirements is through an individual minimum capital ratio (IMCR). The OCC may issue an IMCR in situations in which the OCC determines that significant risks are present that could adversely affect the adequacy of the bank's capital. Through the IMCR, the OCC may require the bank to achieve and maintain capital levels higher than regulatory minimums and to submit a capital plan when the bank's capital levels are below the levels required by the IMCR.

Formal Enforcement Actions

Formal Agreement

Similar to an MOU and a commitment letter, a formal agreement requires agreement between the OCC and the bank about the action necessary to correct the identified problems. The OCC proposes a formal agreement when management is cooperative and the problems are not so severe that a C&D order, as explained later in this book, is warranted. A formal agreement differs from an informal agreement in that a formal agreement is a public document and the OCC may assess CMPs for any violation of that agreement.[115] In addition, the OCC may order compliance with a formal agreement through a C&D order. A composite CAMELS rating of 3 or lower

---

[113] For more information, refer to 12 USC 1831p-1, "Standards for Safety and Soundness," and 12 CFR 30, "Safety and Soundness Standards."

[114] For more information, refer to 12 CFR 3, "Capital Adequacy Standards," and the OCC's *New Capital Rule Quick Reference Guide for Community Banks.*

[115] All formal enforcement actions are public documents.

creates a presumption for a formal enforcement action (either a formal agreement or a C&D order).

Orders Under 12 USC 1818

Through a C&D order, the OCC may fashion appropriate remedies for violations of law or unsafe or unsound banking practices. The OCC may use a C&D order to require banks to stop certain practices and to take affirmative action to correct conditions resulting from the violations or practices at issue. The OCC issues C&D orders typically when the agency is not confident that bank management has the ability or willingness to take the necessary corrective action, or when the problems are so severe that the OCC cannot justify a lesser action.

When the OCC determines that a C&D order is required, the agency brings the problems to the board's attention and presents the directors with an order specifying the necessary corrective actions. Usually, the OCC presents the order at a board meeting. At that time, the OCC asks for the board's consent to the order. "Consent order" is the title given by the OCC to a C&D order that the bank enters into voluntarily, and it becomes final by the board's execution on behalf of the bank of a stipulation and consent document. Once an order becomes effective, all directors are responsible for compliance with it. A C&D order remains in effect until the OCC terminates it.

If the OCC does not obtain board consent to a C&D order, the OCC may decide to serve a notice of charges setting forth the basis for the action. A notice of charges typically is a public document. The bank must file an answer to the charges contained in the notice, after which the matter proceeds to a formal administrative hearing.

The Administrative Procedure Act specifies that an administrative hearing be held on the charges before an independent administrative law judge. The hearing typically is open to the public, and the OCC has the burden of proving the charges in the notice of charges by a preponderance of the evidence. After the hearing and the filing of briefs by counsel, the administrative law judge files a recommended decision. The Comptroller of the Currency then reviews the entire case, with the assistance of agency counsel who was not involved in the administrative action, and renders a final agency decision. If the Comptroller's decision is unfavorable to the bank and results in the issuance of a C&D order, the bank can appeal the case to a U.S. Court of Appeals.

If a bank fails to comply with a C&D order, the OCC can take the matter to federal district court to seek a mandatory injunction requiring compliance. If the bank does not obey the injunction, the OCC can pursue contempt of court proceedings. Moreover, a willful violation of a final C&D order is itself grounds for receivership, and violation of substantial safety and soundness articles in a C&D order can help establish the unsafe or unsound practices or condition that is an element of several other receivership grounds. The OCC also has the authority to impose CMPs or take other administrative action against any individual officer, director, or other IAP who, directly or indirectly, engaged in or participated in the violation.

The OCC can issue a temporary C&D order before a C&D proceeding is completed. This issuance may occur when the OCC determines that such immediate action is necessary to protect the bank, and when the alleged misconduct, or its continuation, would likely cause the bank to become insolvent, cause a significant dissipation of bank assets or earnings, weaken the bank's condition, or prejudice the interests of the depositors. The OCC also may issue a temporary C&D order if a bank's books and records are so incomplete or inaccurate that the agency cannot determine the financial condition of the bank or the details or purpose of any material transaction through the normal supervisory process. A temporary C&D order may require the bank to cease and desist from the violation or practice or to take affirmative corrective action. A bank has 10 days to appeal a temporary C&D order to a federal district court. A temporary C&D order, however, is effective upon service and remains in effect until the administrative proceedings concerning the C&D order are complete, unless a court order sets it aside or the OCC terminates the order.

Capital Directive

As previously noted, a regulation establishes minimum capital requirements for all banks, and the OCC may establish higher capital requirements than required by regulation.[116] If a bank fails to achieve or maintain its minimum capital requirements, the OCC may issue a capital directive against the bank. If the OCC decides to issue a capital directive, it notifies the bank and solicits and carefully reviews the bank's views. If the OCC issues a capital directive, it sets forth in writing the reasons for issuing such an order. The capital directive becomes effective upon issuance. The OCC may enforce a capital directive, or any plan the bank submits to comply with it, to the same extent as a C&D order. Unlike a C&D order, however, a willful violation of or other failure to meet a capital directive is not itself grounds for receivership.

A capital directive, once issued, may require the bank to comply with any or all of the following:

- Achieve the minimum capital level applicable to it.
- Adhere to a preexisting plan to achieve the requisite capital level.
- Submit and adhere to a new capital plan.
- Take other actions, such as reducing assets or dividends, to restore the level of the bank's capital.

Prompt Corrective Action Directive

By law, the OCC and other banking agencies are required to establish five levels of capitalization for insured banks: well capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized.[117] The statute authorizes, and sometimes requires, the OCC to impose a wide range of requirements or restrictions on banks failing to maintain adequate capital, by issuing a PCA directive.

---

116 For more information, refer to 12 CFR 3, "Capital Adequacy Standards."

117 For more information, refer to 12 USC 1831o and 12 CFR 6, "Prompt Corrective Action."

Unless there are immediate time constraints, the OCC notifies a bank in advance of its intention to impose discretionary PCA restrictions and gives the bank an opportunity to submit its views on the matter. If the OCC decides to issue a PCA directive, the directive is enforceable in federal district court, and failure to submit or implement a capital restoration plan required in a PCA directive is grounds for receivership.

Safety and Soundness Order

The OCC has the authority to require compliance with safety and soundness standards.[118] These safety and soundness standards cover internal controls and information systems, internal audits, loan documentation, credit underwriting, interest rate exposure, asset growth, asset quality, earnings, compensation, information security, residential mortgage lending, and, for certain banks, heightened standards.

The OCC may require the bank to submit a compliance plan that specifies how the bank will correct the deficiency. If the bank fails to submit or implement such a plan, the OCC may issue a safety and soundness order requiring the bank to take certain steps to correct the deficiencies. The OCC can enforce the order in federal district court. A willful violation of a safety and soundness order is not itself grounds for receivership, but violation of substantial articles in a safety and soundness order may establish the unsafe or unsound practices or condition that is an element of several receivership grounds.

Other Administrative Actions

Civil Money Penalty

The OCC may assess a CMP of varying amounts against a bank, a director, or another IAP for a violation of any law or regulation, temporary or permanent C&D order, condition imposed in writing, or written agreement. In certain instances, the OCC may assess a CMP for unsafe or unsound banking practices that are reckless and for breaches of fiduciary duty.

When determining whether to bring a CMP action and the amount of the assessment, the OCC considers the following factors:

- The gravity of the violation
- Any history of previous violations
- Evidence of good faith
- The bank’s or IAP’s ability to pay
- Other matters as justice may require

The OCC has broad discretion to determine the amount of a CMP, which permits the agency to tailor the assessment to the facts of each case. For example, the OCC may assess the bank or IAP up to $7,500 a day for violations of any law or regulation, temporary or permanent C&D order,

118 For more information, refer to 12 CFR 30, “Safety and Soundness Standards.”

condition imposed in writing, or written agreement. In certain circumstances, the OCC may assess a CMP of up to $37,500 a day for

- violations of law, regulation, or enforcement action.
- any unsafe or unsound banking practice engaged in recklessly.
- any breach of fiduciary duty.

The OCC also has the authority to assess a CMP of $1,425,000 on a daily basis. These assessments can take place when the bank or IAP knowingly engaged in any violation, practice, or breach and, as a result of that conduct, knowingly or recklessly caused a substantial loss to the bank or knowingly or recklessly received a substantial gain or other benefit.

When determining the amount of a CMP assessment, the OCC takes into account the extent to which the bank has suffered a loss or the bank or IAP has received personal gain from the violation. In addition, the OCC considers any mitigating factors, such as good faith, cooperation, or voluntary reimbursement for losses incurred by a bank or its customers. Conversely, the OCC may impose a more substantial penalty if a bank or IAP fails to cooperate with the OCC, fails to correct the violation, conceals the violation, or shows bad faith.

Before deciding whether to assess a CMP, the OCC gives the bank or IAP an opportunity to submit written information about the alleged violation as well as the specific factors the OCC should consider when reviewing the case. After thoroughly reviewing the written response and analyzing the case, the OCC sends the individual a no-action letter, a supervisory letter, a letter of reprimand, or a notice of assessment. Supervisory letters and letters of reprimand state that no assessment will be imposed but advise that a future violation may result in a CMP assessment by the OCC.

If the OCC issues a CMP notice of assessment, the bank or IAP must request a formal agency hearing, or the notice of assessment becomes final. The hearing and appeal procedures to review a CMP are the same as those for a C&D order.

Conservatorship and Receivership

In severe cases, the OCC has the authority to place a bank into conservatorship or receivership. In a conservatorship, a conservator selected by the OCC manages the bank until the agency determines what action to take. In a receivership, the OCC closes the bank immediately and hands it over to the receiver, which is typically the FDIC.

Other Actions

The OCC may pursue other actions against banks that conduct securities activities subject to the Securities Exchange Act.[119] Such securities activities—including acting as a broker-dealer, a government securities broker-dealer, a municipal securities dealer, or a transfer agent—may be performed by a bank or its operating subsidiary. The OCC has authority under the Securities

[119] For more information, refer to 15 USC 78a et seq., "Securities Exchange Act of 1934."

Exchange Act to take action to redress certain violations of the federal securities laws by banks and associated persons that the OCC supervises. Depending on the severity of the violation, the OCC may censure a bank that has engaged in improper activities. The OCC may deny or revoke a bank's registration for certain securities activities, thereby affecting the bank's ability to engage in such activities, or it may limit or suspend certain securities activities. The OCC may use these actions alone or in combination with other administrative remedies.

Actions Against Individuals

The OCC has the authority to undertake certain administrative actions against individual bank directors or other IAPs. The agency may choose to take action if a director or other IAP

- violates any law, rule, or regulation, or outstanding agency order, agreement, or condition imposed in writing.
- engages in an unsafe or unsound banking practice or breaches a fiduciary duty.

The actions available to the OCC include a C&D order, a CMP, and a removal or prohibition action. These tools may require a director or other IAP to refrain from taking certain actions, or they may require the director or other IAP to take certain affirmative actions (such as making restitution or correcting the problem).

Cease-and-Desist Order

The OCC may request a director or other IAP who has engaged in a violation or an unsafe or unsound banking practice to consent to a C&D order. The order might require the director or other IAP to take certain actions to correct the conditions that resulted from the violation or practice. It also might require the director or other IAP to reimburse the bank for losses resulting from the misconduct and might restrict the director's or other IAP's activity regarding the conduct at issue.

If the director or other IAP declines to enter into the order on a consensual basis and cannot reach a settlement with the OCC, the agency may issue a notice of charges against the individual. This notice is public. The notice seeks the formal issuance of a C&D order and must set forth the specific charges against the director or other IAP. In addition, the OCC must base issuance of the notice on one or more of the following:

- A violation of law, rule, or regulation
- A violation of a condition imposed in writing by the agency in connection with the granting of an application
- A violation of a formal agreement previously entered into
- An unsafe or unsound banking practice

The individual must file an answer to the charges contained in the notice, after which the matter proceeds to a formal administrative hearing in the same fashion as described previously with regard to administrative actions against banks.

Prohibition or Removal and Suspension

The OCC may initiate action to prohibit and remove a bank director or other IAP from banking in cases in which particularly serious misconduct has occurred. In addition, the OCC may seek to prohibit a former director or other IAP as described more fully below. The OCC must base prohibition and removal actions on the following statutory elements, which address conduct, effect, and culpability:

- The individual must have engaged in or committed one or more of the following:
  - A violation of law, rule, or regulation
  - A violation of a condition imposed in writing by the agency in connection with the granting of an application
  - A violation of an outstanding formal agreement or C&D order
  - An unsafe or unsound banking practice
  - A breach of fiduciary duty
- The conduct described above must have resulted in
  - a loss or potential loss or other damage to a bank or business institution,
  - a financial gain or other benefit to the individual, or
  - prejudice or potential prejudice to the interests of the depositors.
- The individual's culpability for the conduct described must include either
  - personal dishonesty, or
  - willful or continuing disregard for the safety and soundness of the bank.

The hearing process for a prohibition or removal action is identical to a C&D hearing process. If adverse to the individual, the individual may appeal the agency's decision to a U.S. Court of Appeals.

Once in place, a prohibition or removal order prohibits the individual from participating in any manner in the conduct of any bank's affairs, participating in voting for a bank director, or serving or acting as a director, officer, employee, or other IAP. The removal or prohibition order applies to all federally insured depository institutions and their holding companies (which can include banks, savings associations, credit unions, and farm credit institutions) and to all federal bank regulatory agencies.

Both the agency issuing the removal or prohibition order and the agency supervising the financial institution with which the removed or prohibited individual is seeking to become affiliated must grant any exception to the restrictions of a prohibition or removal order.

Once the OCC initiates a removal action, but before finalizing it, the agency may issue a suspension order against the individual. This order temporarily removes the individual from the banking industry to the same extent as a final removal order. The OCC takes such action, however, only if the agency determines that the action is necessary to protect the bank or its depositors. The suspended individual has the right to seek a stay of a suspension order from a federal district court within 10 days of the service of the suspension order. The suspension order is effective upon service by the OCC and remains in effect until the removal proceedings are completed, the OCC dismisses the charges, the agencies grant a written waiver, or a court stays the order.

If a director or other IAP is indicted or charged with a felony involving dishonesty or breach of trust, or with a violation of the AML statutes, the OCC also may suspend the individual. The OCC must first determine that the individual's continued service or affiliation with the bank may threaten the depositors' interests or may impair public confidence in any relevant depository institution. The suspended individual may request an informal hearing before the agency to modify or terminate the suspension order. The suspension remains in effect until the OCC terminates it, or until the criminal charges are resolved.

If a director or other IAP is convicted of any offense involving dishonesty, breach of trust, or money laundering, the individual is removed automatically from the banking industry. Under certain circumstances, the individual may petition the FDIC for permission to reenter banking.

Appeals Process

The OCC desires consistent and equitable supervision and seeks to resolve disputes that arise during the supervisory process fairly and expeditiously in an informal, amicable manner. Banks are encouraged to contact the OCC ombudsman to discuss any agency policy, decision, or action that might develop into an appealable matter. The ombudsman's objective in these cases is to seek a resolution to the dispute before it develops into an appeal. If banks cannot resolve disagreements through this discussion, they are encouraged to file an appeal with the applicable supervisory office or the ombudsman[120] to seek a further review of the decisions or actions in dispute.

Functioning as an independent advisor and decision maker, the ombudsman can accept appeals related to, for example, examination ratings, the adequacy of loan loss reserve positions, and loan classifications. The ombudsman may not accept, for example, appeals related to

- the appointment of receivers and conservators.
- preliminary examination conclusions communicated to a bank before a final report of examination is issued.
- enforcement-related actions or decisions.
- formal and informal rulemakings pursuant to the Administrative Procedure Act.
- requests for information filed under the Freedom of Information Act.

With the prior consent of the Comptroller of the Currency, the ombudsman may stay an appealable agency decision or action during the resolution of an appealable matter.

[120] For more information on the appeals process, refer to the "Bank Appeals" page on the OCC's website.

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.

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.[121]	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.[122]	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.[123]
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	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

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

[122] Ibid.

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

National banks	FSAs
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.	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 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.[124]
Attorney	
No similar prohibition.	Not more than one director may be an attorney with a particular law firm.[125]
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.[126]	A director of a stock FSA need not be a stockholder of the FSA unless the bylaws so require.[127] A director of a mutual FSA is required to be a member of the FSA.[128]
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.[129]	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.[130]	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.[131]

[124] For more information, refer to 12 CFR 163.201, "Corporate Opportunity."

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

[126] For more information, refer to 12 USC 72 and 12 CFR 7.2005, "Ownership of Stock Necessary to Qualify as Director."

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

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

[129] 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."

[130] 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."

[131] 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.[132]
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.[133]
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.[134]	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.[135]
Committee member requirements	
Refer to the “Establish and Maintain an Appropriate Board Structure” section of this book.	Refer to the “Establish and Maintain an Appropriate Board Structure” section of this book.

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

[133] Ibid.

[134] For more information, refer to 12 USC 71, “Election,” and 12 CFR 7.2024.

[135] 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.

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.[136]		
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 book.	Officers serve at will.[137]	The board must approve all employment contracts and compensation arrangements for senior officers and directors.[138]
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	An FSA must adopt and follow written policies and procedures adequate to maintain its fiduciary activities in

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

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

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

Policy	National banks and FSAs	National banks only	FSAs only
		administration of a fiduciary account, except with the specific approval of the board.[139] A national bank's asset management activities shall be managed by or under the direction of its board.[140] 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.[141]	compliance with applicable law.[142] The exercise of fiduciary powers must be managed by or under the direction of the board.[143]
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.[144]
Heightened standards.	Banks with average total consolidated assets of $50 billion or greater or those that are OCC-		

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

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

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

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

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

[144] For more information, refer to 12 CFR 163.172.

Policy	National banks and FSAs	National banks only	FSAs only
	designated, which are referred to as covered banks, should have robust governance as outlined in the guidelines.[145]		
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.[146]		
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.[147]		
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.[148]		

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

[146] 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."

[147] For more information, refer to 12 CFR 30, appendix B.

[148] 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.[149]		An FSA 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. 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.[150]
Real estate lending standards, interagency, and supplemental lending limits.		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.[151]	The board must, at least annually, review and approve written policies that establish appropriate limits and standards for extensions of credit that are

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

[150] For more information, refer to 12 CFR 163.176.

[151] For more information, refer to 12 CFR 34.62, subpart D, appendix A, "Interagency Guidelines for Real Estate Lending."

Policy	National banks and FSAs	National banks only	FSAs only
		A bank eligible to participate in the pilot program for residential real estate and small business loans must submit an application that includes a written resolution by a majority of the directors approving higher lending limits as described in (a)(1), (2), and (3) of the regulation.[152]	secured by real estate.[153]
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.[154]	Two directors must attest to the report's correctness.[155]
Safe and sound banking practices.	The board must oversee the bank's compliance with safe and sound banking practices.[156]		
Security program and designation of a security officer.	The board must ensure that the bank has a written security program		

[152] For more information, refer to 12 CFR 32.7(b)(3), "Application Process."

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

[154] For more information, refer to 12 USC 161, "Reports to Comptroller of the Currency," and 12 USC 1817(a)(3), "Reports of Condition; Access to Reports."

[155] For more information, refer to 12 USC 1464(v), "Reports of Condition," and 12 USC 1817(a)(3), "Reports of Condition; Access to Reports."

[156] For more information, refer to 12 CFR 30, "Safety and Soundness Standards."

Policy	National banks and FSAs	National banks only	FSAs only
	for the main and branch offices. The board must designate a security officer to report at least annually on the implementation, administration, and effectiveness of the security program.[157]		
Specific funds availability.	To meet the requirements of a specific availability policy disclosure under 12 CFR 229.17 and 12 CFR 229.18(e), a bank shall provide a disclosure describing the bank's policy on when funds deposited in an account are available for withdrawal.[158]		
Disclosure requirements related to capital requirements.	In general, under both regulations, the board must approve the bank's formal disclosure policy that addresses the bank's approach for determining the disclosures it should make.[159]		

[157] For national banks, refer to 12 CFR 21, subpart A, "Minimum Security Devices and Procedures." For FSAs, refer to 12 CFR 168, "Security Procedures."

[158] 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."

[159] For more information, refer to 12 CFR 3.62, "Disclosure Requirements," and 12 CFR 3.172, "Disclosure Requirements."

Appendix C: 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 establish and make decisions about the bank's strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits through 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 ensure that all material risks and associated risk concentrations are identified, measured, monitored, and controlled.

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 D: Abbreviations

AML	anti-money laundering
BOLI	bank-owned life insurance
BSA	Bank Secrecy Act
C&D	cease-and-desist
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
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
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FSA	federal savings association
GLBA	Gramm–Leach–Bliley Act
IAP	institution-affiliated party
IMCR	individual minimum capital ratio
IRM	independent risk management
IT	information technology

LBS	Large Bank Supervision
MCBS	Midsize and Community Bank Supervision
MIS	management information systems
MOU	memorandum of understanding
MRA	matter requiring attention
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
PCA	prompt corrective action
USC	U.S. Code

Appendix E: References

Laws

Title 12, “Banks and Banking”
12 USC 22, “Organization Certificate” (national banks)
12 USC 24, “Corporate Powers of Associations” (national banks)
12 USC 56, “Prohibition on Withdrawal of Capital; Unearned Dividends” (national banks)
12 USC 60, “National Bank Dividends” (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 75, “Legal Holiday, Annual Meeting On; Proceedings Where No Election Held on Proper Day” (national banks)
12 USC 76, “President of Bank as Member of Board; Chairman of Board” (national banks)
12 USC 84, “Lending Limits” (national banks and federal savings associations)
12 USC 90, “Depositaries of Public Moneys and Financial Agents of Government” (national banks)
12 USC 92a, “Trust Powers” (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 222, “Federal Reserve Districts; Membership of National Banks” (national banks)
12 USC 371c, “Banking Affiliates” (national banks and federal savings associations)
12 USC 371c-1, “Restrictions on Transactions With Affiliates” (national banks and federal savings associations)
12 USC 375a, “Loans to Executive Officers” (national banks and federal savings associations)
12 USC 375b, “Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Member Banks” (national banks and federal savings associations)
12 USC 481, “Appointment of Examiners; Examination of Member Banks, State Banks, and Trust Companies; Reports” (national banks)
12 USC 484, “Limitation on Visitorial Powers” (national banks)
12 USC 1463, “Supervision of Savings Associations” (federal savings associations)
12 USC 1464, “Federal Savings Associations” (federal savings associations)
12 USC 1468, “Transactions With Affiliates; Extensions of Credit to Executive Officers, Directors, and Principal Shareholders” (federal savings associations)

12 USC 1815, "Deposit Insurance" (national banks and federal savings associations)
12 USC 1817, "Assessments" (national banks and federal savings associations)
12 USC 1818, "Termination of Status as Insured Depository Institution" (national banks and federal savings associations)
12 USC 1820, "Administration of Corporation" (national banks and federal savings associations)
12 USC 1821, "Insurance Funds" (national banks and federal savings associations)
12 USC 1828(z), "General Prohibition on Sale of Assets" (national banks and federal savings associations)
12 USC 1831i, "Agency Disapproval of Directors and Senior Executive Officers of Insured Depository Institutions or Depository Institution Holding Companies" (national banks and federal savings associations)
12 USC 1831m, "Early Identification of Needed Improvements in Financial Management" (national banks and federal savings associations)
12 USC 1831o, "Prompt Corrective Action" (national banks and federal savings associations)
12 USC 1831p-1, "Standards for Safety and Soundness" (national banks and federal savings associations)
12 USC 1861 et seq., "Bank Service Companies" (national banks and federal savings associations)
12 USC 1971, "Definitions" (national banks)
12 USC 1972, "Certain Tying Arrangements Prohibited; Correspondent Accounts" (national banks: "Tying Arrangements") (national banks and federal savings associations: "Correspondent Accounts")
12 USC 1972, "Certain Tying Arrangements Prohibited; Correspondent Accounts" (national banks)
12 USC 2901 et seq., "Community Reinvestment" (national banks and federal savings associations)
12 USC 3201 et seq., "Depository Institutions Management Interlocks" (national banks and federal savings associations)
15 USC 2, "Monopolizing Trade a Felony; Penalty" (national banks and federal savings associations)
15 USC 77a et seq., "Securities and Trust Indentures" (national banks and federal savings associations)
15 USC 77jjj, "Eligibility and Disqualification of Trustee" (national banks and federal savings associations)
15 USC 78a et seq., "Securities Exchange Act of 1934" (national banks and federal savings associations)
15 USC 78dd-1 et seq., "Foreign Corrupt Practices Act of 1977" (national banks and federal savings associations)
15 USC 78j-1, "Audit Requirements" (national banks and federal savings associations)
15 USC 78n-2, "Corporate Governance" (national banks and federal savings associations)
15 USC 78u-6, "Securities Whistleblower Incentives and Protection" (national banks and federal savings associations)

18 USC 215, "Receipt of Commissions or Gifts for Procuring Loans" (national banks and federal savings associations)
18 USC 656, "Theft, Embezzlement, or Misapplication by Bank Officer or Employee" (national banks and federal savings associations)
18 USC 1001, "Statements or Entries Generally" (national banks and federal savings associations)
18 USC 1005, "Bank Entries, Reports, and Transactions" (national banks and federal savings associations)
18 USC 1344, "Bank Fraud" (national banks and federal savings associations)
29 USC 1001, "Congressional Findings and Declaration of Policy" (national banks and federal savings associations)
52 USC 30101 et seq., "Federal Election Campaign Act of 1971" (national banks and federal savings associations)

Regulations

11 CFR 100, subpart B, "Definition of Contribution" (national banks and federal savings associations)
11 CFR 114, "Corporate and Labor Organization Activity" (national banks and federal savings associations)
12 CFR 3, "Capital Adequacy Standards" (national banks and federal savings associations)
12 CFR 4, "Organization and Functions, Availability and Release of Information, Contracting Outreach Program, Post-Employment Restrictions for Senior Examiners" (national banks and federal savings associations)
12 CFR 5, "Rules, Policies, and Procedures for Corporate Activities" (national banks and federal savings associations)
12 CFR 6, "Prompt Corrective Action" (national banks and federal savings associations)
12 CFR 7, "Bank Activities and Operations" (national banks: all provisions; federal savings associations: 12 CFR 7.1000, 12 CFR 7.3001, and 12 CFR 7.4010)
12 CFR 8, "Assessment of Fees" (national banks and federal savings associations)
12 CFR 9, "Fiduciary Activities of National Banks" (national banks)
12 CFR 11, "Securities Exchange Act Disclosure Rules" (national banks)
12 CFR 21, "Minimum Security Devices and Procedures, Reports of Suspicious Activities, and Bank Secrecy Act Compliance Program" (national banks: subparts A and B; national banks and federal savings associations: subpart C)
12 CFR 21.21 (c)(2) "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance—Customer Identification Program" (national banks and federal savings associations)
12 CFR 25, "Community Reinvestment Act and Interstate Deposit Production Regulations" (national banks)
12 CFR 26, "Management Official Interlocks" (national banks and federal savings associations)
12 CFR 30, "Safety and Soundness Standards" (national banks and federal savings associations)

12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness" (national banks and federal savings associations)
12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards" (national banks and federal savings associations)
12 CFR 30, appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches" (national banks and federal savings associations)
12 CFR 31, "Extensions of Credit to Insiders and Transactions With Affiliates" (national banks)
12 CFR 32, "Lending Limits" (national banks and federal savings associations)
12 CFR 34, "Real Estate Lending and Appraisals" (national banks: subparts A, B, D, and E; national banks and federal savings associations: subparts C and G)
12 CFR 41, "Fair Credit Reporting" (national banks and federal savings associations)
12 CFR 46, "Annual Stress Test" (national banks and federal savings associations)
12 CFR 145, "Federal Savings Associations—Operations" (federal savings associations)
12 CFR 150, "Fiduciary Powers of Federal Savings Associations" (federal savings associations)
12 CFR 160, "Lending and Investment" (federal savings associations)
12 CFR 163, "Savings Associations—Operations" (federal savings associations)
12 CFR 168, "Security Procedures" (federal savings associations)
12 CFR 195, "Community Reinvestment" (federal savings associations)
12 CFR 206, "Limitations on Interbank Liabilities (Regulation F)" (national banks and federal savings associations)
12 CFR 215, "Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (Regulation O)" (national banks and federal savings associations)
12 CFR 223, "Transactions Between Member Banks and Their Affiliates (Regulation W)" (national banks and federal savings associations)
12 CFR 229, "Availability of Funds and Collection of Checks (Regulation CC)" (national banks and federal savings associations)
12 CFR 327, "Assessments" (national banks and federal savings associations)
12 CFR 359, "Golden Parachute and Indemnification Payments" (national banks and federal savings associations)
12 CFR 363, "Annual Independent Audits and Reporting Requirements" (national banks and federal savings associations)
17 CFR 240.21(F-1) et seq., "Whistleblower Status and Retaliation Protection" (national banks and federal savings associations)
31 CFR 1020.210, "Anti-Money Laundering Program Requirements for Financial Institutions Regulated by Only a Federal Functional Regulator, Including Banks, Savings Associations, and Credit Unions" (national banks and federal savings associations)

Comptroller's Handbook

Asset Management

"Asset Management" (national banks and federal savings associations)
"Retirement Plan Products and Services" (national banks and federal savings associations)

Consumer Compliance

"Community Reinvestment Act Examination Procedures" (national banks)
"Compliance Management System" (national banks and federal savings associations)

Examination Process

"Bank Supervision Process" (national banks and federal savings associations)
"Community Bank Supervision" (national banks and federal savings associations)
"Federal Branches and Agencies Supervision" (national banks and federal savings associations)
"Large Bank Supervision" (national banks and federal savings associations)

Management

"Corporate and Risk Governance" (national banks and federal savings associations)

Safety and Soundness

"Insider Activities" (national banks and federal savings associations)
"Internal and External Audits" (national banks)
"Internal Controls" (national banks)
"Liquidity" (national banks and federal savings associations)
"Related Organizations" (national banks)

OTS Handbook

Office of Thrift Supervision Examination Handbook (federal savings associations)

Section 340, "Internal Control"
Section 350, "External Audit"
Section 355, "Internal Audit"
Section 730, "Related Organizations"
Section 760, "New Activities and Services"
Section 1500, "Community Reinvestment Act"

OCC Issuances

Banking Bulletin 1992-42, "Interagency Policy Statement: External Auditors" (August 3, 1992) (national banks and federal savings associations)

A Common Sense Approach to Community Banking

Director's Toolkit: Detecting Red Flags in Board Reports: A Guide for Directors (February 2004)

Director's Toolkit: Internal Controls: A Guide for Directors (September 2000)

Director's Toolkit: Pocket Guide to Detecting Red Flags in Board Reports (October 2003)

New Capital Rule Quick Reference Guide for Community Bankers

OCC Bulletin 1999-37, "Interagency Policy Statement on External Auditing Programs: External Audit" (October 7, 1999) (national banks and federal savings associations)

OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing" (March 17, 2003) (national banks and federal savings associations)

OCC Bulletin 2003-38, "Removal, Suspension, and Debarment of Accountants From Performing Annual Audit Services: Publication of Final Rule" (September 3, 2003) (national banks)

OCC Bulletin 2004-20, "Risk Management of New, Expanded, or Modified Bank Products and Services: Risk Management Process" (May 10, 2004) (national banks)

OCC Bulletin 2004-56, "Bank-Owned Life Insurance: Interagency Statement on the Purchase and Risk Management of Life Insurance" (December 7, 2004) (national banks and federal savings associations)

OCC Bulletin 2007-31, "Prohibition on Political Contributions by National Banks: Updated Guidance" (August 24, 2007) (national banks)

OCC Bulletin 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies" (June 30, 2012) (national banks and federal savings associations)

OCC Bulletin 2012-14, "Stress Testing: Interagency Stress Testing Guidance" (May 14, 2012) (national banks and federal savings associations)

OCC Bulletin 2012-16, "Capital Planning: Guidance for Evaluating Capital Planning and Adequacy" (June 7, 2012) (national banks and federal savings associations)

OCC Bulletin 2012-33, "Community Bank Stress Testing: Supervisory Guidance" (October 18, 2012) (national banks and federal savings associations)

OCC Bulletin 2013-29, "Third-Party Relationship: Risk Management Guidance" (October 30, 2013) (national banks and federal savings associations)

OCC Bulletin 2014-5, "Dodd–Frank Stress Testing: Supervisory Guidance for Banking Organizations With Total Consolidated Assets of More Than $10 Billion but Less Than $50 Billion" (March 5, 2014) (national banks and federal savings associations)

OCC Bulletin 2014-35, "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations" (July 22, 2014) (mutual federal savings associations)
OCC Bulletin 2014-52, "Matters Requiring Attention: Updated Guidance" (October 30, 2014) (national banks and federal savings associations)
OCC Bulletin 2015-30, "Standards for Assessing the Diversity Policies and Practices of Regulated Entities: Final Interagency Policy Statement" (June 24, 2015) (national banks and federal savings associations)

Other

Comptroller's Licensing Manual

"Background Investigations"
"Changes in Directors and Senior Executive Officers"
"Management Interlocks"

Basel Committee on Banking Supervision

"The Internal Audit Function in Banks" (December 2011)
"Principles for Effective Risk Data Aggregation and Risk Reporting" (January 2013)
"External Audits of Banks" (March 2014)
"Corporate Governance Principles for Banks" (July 2015)

FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual

FFIEC Information Technology Examination Handbook

"Business Continuity Planning"
"Management"
"Outsourcing Technology Services"

RESCINDED