November 2020

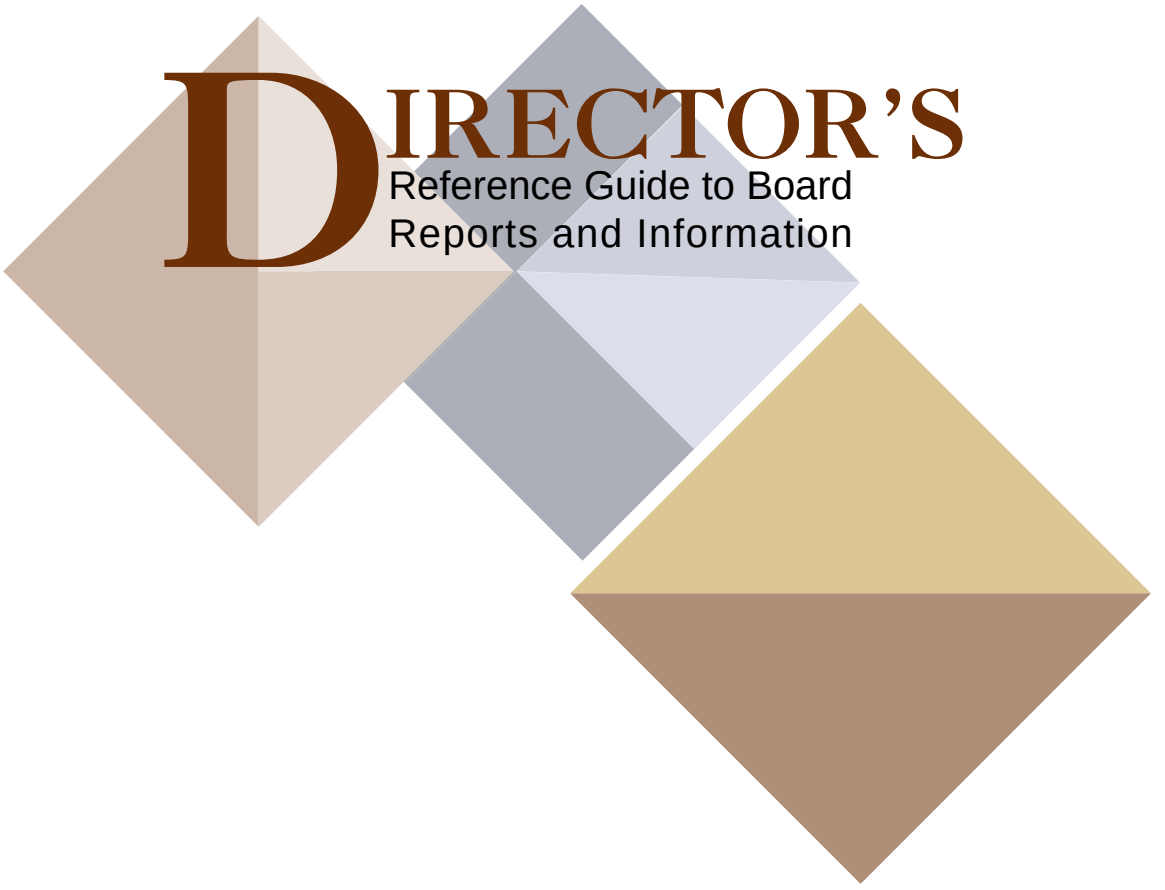
As of March 2025, the OCC no longer examines for reputation risk. This publication has been updated.

Office of the Comptroller of the Currency

DIRECTOR'S

Reference Guide to Board Reports and Information

As of March 2025, references to reputation risk have been removed from this publication. Refer to OCC Bulletin 2025-4. Pages in this book where reputation risk references were removed are indicated by text in the top margin.



DIRECTOR'S

Reference Guide to Board Reports and Information

Office of the Comptroller of the Currency
November 2020

Contents

Preface

The *Director's Reference Guide to Board Reports and Information* (Director's Reference Guide) is for boards of directors of national banks and federal savings associations (collectively, banks) to assist directors in fulfilling their corporate governance responsibilities.[1] When it is necessary to distinguish between national banks and federal savings associations (FSA), they are referred to separately.

Sound decisions begin with timely, accurate, relevant, and complete information. A bank's board of directors needs concise and relevant reports from a variety of sources to carry out its oversight responsibilities. Board oversight is critical to maintaining the bank's operations in a safe and sound manner and the bank's compliance with laws and regulations. Effective board oversight includes overseeing banking activities and senior management. Directors should receive sufficient and transparent information from bank management to fulfill their oversight and fiduciary duties. A director may be held personally liable and be subject to monetary penalties or other sanctions for breaching such duties.[2]

The Director's Reference Guide supplements other publications by the Office of the Comptroller of the Currency (OCC). These include the *Director's Book: Role of Directors for National Banks and Federal Savings Associations* (Director's Book) and booklets of the *Comptroller's Handbook*. The Director's Book provides an overview of the OCC, highlights OCC resources available to directors, outlines directors' responsibilities as well as management's role, explains basic concepts and standards for the safe and sound operation of banks, and delineates laws and regulations that apply to banks. Although *Comptroller's Handbook* booklets are written for examiners, directors may refer to them, including the "Corporate and Risk Governance" booklet, to better understand a particular bank activity and its associated risks.

The Director's Reference Guide does not create rights or legal protections for banks or directors, or create obligations for the OCC. This guide is not all-inclusive and does not cover all topics that directors should be knowledgeable about or that directors should receive information on to

[1] The corporate governance provisions discussed in the Director's Reference Guide are not intended to, nor do they, exceed applicable state law requirements.

[2] A director who violates any banking law or regulation, engages in an unsafe or unsound banking practice, breaches a fiduciary duty, or knowingly allows another to do so may be held personally liable or subjected to monetary penalties or other sanctions. For more information, refer to 12 USC 1818(e), "Removal and Prohibition Authority" and 1818(i)(2), "Civil Money Penalty."

perform their duties. The types, amount, and frequency of information that directors should receive to effectively perform their duties varies at each bank and continually evolves. Directors should understand what information they need to fulfill their oversight obligations.

For purposes of the Director's Reference Guide, the term "board," unless otherwise stated, refers to the board or a board-designated committee that is primarily responsible for providing effective oversight. The term "senior management" refers to bank employees designated by the board as executives responsible for making key decisions. Senior management may include the president, chief executive officer, chief financial officer, chief risk executive,[3] chief information officer, chief compliance officer, chief credit officer, chief audit executive,[4] and chief bank counsel. Titles and positions may vary depending on the bank's structure, size, and complexity. The term "management" refers to bank managers responsible for carrying out the bank's day-to-day activities.

The OCC intends to periodically review and update the Director's Reference Guide. When the OCC makes changes to the Director's Reference Guide, the agency will publish an OCC bulletin to announce the updated version to the general public. To receive OCC bulletins by email, directors should sign up for the OCC's email listserv.

Heightened Standards

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

[3] A chief risk executive is also commonly known as a chief risk officer.

[4] A chief audit executive is also commonly known as a chief auditor.

Introduction

The board of directors' role is to oversee the bank's activities, provide credible challenge to management, and hold management accountable.[5] To help perform these duties, the board should receive information from a range of sources in a useful and readable format. The information requirements, particularly the number, variety, and sources of reports, depend on the bank's size, complexity, operations, risks, and issues. The board should work with management to determine what information and format the board needs—financial and nonfinancial and from whom—to perform its duties effectively. Some sources of information include senior management, board committees, management committees, external experts or advisors, risk management and compliance personnel, internal and external auditors, and regulators. The board's information requirements should evolve as the bank grows in size and complexity or the bank's risk profile changes.

Sections of the Director's Reference Guide focus on key areas of planning, operations, and risk management. Each section is organized as follows:

- **Sources of information:** Examples of sources of information that directors review when overseeing each key area. The sources of information may vary in title, content, scope, detail, or format but should be commensurate with the bank's size, complexity, risks, and operations to enable effective corporate governance.
- **Measures:** Examples of quantitative information that directors review when overseeing areas discussed in this guide. Measures, including metrics, limits, targets, and indicators, help directors to understand the bank's operations and risks. Common measures compare performance with business unit or bank-wide risk limits to allow directors to assess whether the bank is operating within the board's risk appetite. Examples of measures include key risk indicators (KRI), key performance indicators (KPI), and key control indicators (KCI). KRIs are qualitative or quantitative measures that help to identify changes to existing risks. KPIs are qualitative or quantitative measures used to track and analyze factors deemed critical to the success of an organization. KCIs are qualitative or quantitative measures used to track and analyze factors related to the effectiveness of internal controls. Some of the examples of measures used in this booklet are KRIs, KPIs, or KCIs.

[5] For more information on the board's responsibilities, refer to the Director's Book and the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook*.

- **Questions to consider:** Examples of questions that directors may consider in their oversight of areas discussed in this guide. Active directors pose questions to provide credible challenge[6] to management and make adequately informed decisions.
- **Red flags:** Examples of ratios, trends, or situations indicated in board reports and materials or other information that may signal existing or potential problems in key areas and could warrant further director attention or investigation.
- **References:** References that may assist directors when overseeing each area discussed in this guide.

The board should agree on a set of key performance measurements and risk indicators and work with management to determine the appropriate frequency for reporting information. Management should be transparent and work with the board to determine the best format for the information that the board requires. For example, dashboard-style reports or executive summaries, supplemented by additional material, may enhance report readability. Regardless of the presentation style, information presented to the board should highlight important performance and risk measures, ratios, limits, metrics, variances, and trends rather than raw data or highly technical detail. Directors should understand the reasons for significant variances, breached limits, and increasing risks and should request more information from management as needed.

Directors should receive sufficient information to perform their duties, including understanding and assessing the bank's performance, risk profile, material risks, and significant audit and regulatory issues. Directors should do more than merely review and accept the information presented. Directors should ask questions to gain clarity; request supplemental information, including presentations from management on key topics and issues; and provide credible challenge to management as needed. Directors should identify red flags, which should prompt them to ask for more information and focus additional board and management attention on the matters at hand.

Key financial performance ratios and trends may be found in the quarterly Uniform Bank Performance Report (UBPR), and Canary, while others can be computed from internal bank records. The UBPR and Canary are system-generated reports based on the Consolidated Reports of Condition

[6] Credible challenge is the method that directors use to hold management accountable by being engaged, asking questions, and gaining the information needed, when appropriate, to satisfy themselves that management's strategies are viable and in the bank's best interests.

and Income (call report) data and are available on BankNet.[7] The UBPR can help directors evaluate a bank's current condition, assess trends in financial performance, and compare the bank's performance with its peer group, as well as prompt directors to ask senior management questions or for more information.[8] Canary is an OCC-designed analytical tool used to enhance the identification of emerging credit, interest rate, and liquidity risk of a bank.[9] Canary helps identify banks that are exhibiting or trending toward high-risk positions. The results from Canary—along with other tools—should be evaluated in the context of the bank's overall activities, risk profile, and condition.

Reports on the bank's financial performance should help directors assess the bank's condition and determine whether the bank's risk exposure is within the board's established risk appetite and limits. To use financial information effectively, directors should look at individual and peer performance measures as well as the trend and interrelationships among capital, asset quality, earnings, liquidity, sensitivity to market risk, and balance-sheet changes. Financial reports should focus on comparative financial statements and key financial performance ratios and highlight current and emerging risks. In reviewing these reports, directors should focus on any material item that has changed significantly or that varies significantly from plans or expectations. If deviations are not clearly reflected in the report, directors should ask management to explain the deviations.

---

[7] BankNet is the OCC's secure website for communicating with and receiving information from banks. BankNet is available only to OCC-regulated banks and provides information that is not available 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.

[8] The UBPR shows performance and composition data, is organized by subject, reports data for five separate quarters that tie to the quarterly call report filings, and compares the performance of a bank against itself over time and against the performance of a group of peer banks. A bank's peer group includes banks of similar size, type, and location. For more information, refer to the Federal Financial Institutions Examination Council's *Uniform Bank Performance Report User's Guide*.

[9] The report shows 15 benchmarked measures from two perspectives: a static position and a one-year rate of change. Canary does not flag risk measures for banks with a composite CAMELS rating of 3 or worse when they exceed the benchmark for a risk category. For more information on the composite ratings under the Uniform Financial Institutions Rating System, or CAMELS, refer to the "Bank Supervision Process" booklet of the Comptroller's Handbook. The measures are derived from call report data. Results for the most recent five quarters are displayed on the report.

Each director should review reports and significant communications from the bank's regulators and control functions, including internal and external auditors and independent risk management (IRM).[10] Information from these reports and communications can help the board assess the accuracy and validity of information from management as well as inform directors of deficiencies and emerging risks. Directors should understand any concerns and problems identified and confirm that management executes timely and sustainable corrective actions. Uncorrected supervisory concerns contained in matters requiring attention, violations, or enforcement action articles resulting from the board's failure to oversee the bank appropriately may result in the OCC holding individual directors accountable for lack of corrective action. A director who needs help understanding information or expectations in a report or communication should contact the regulator, the bank's audit committee, auditors, or independent consultants who prepared the report.

[10] Examples of common reports and communications from IRM include results of compliance monitoring, credit risk review reports, and reports of other reviews completed by second line functions.

General

There are red flags that directors should consider in their oversight for all key areas of the bank. In addition to identifying red flags that are readily available and evident in reports, a director needs to understand instances where information needed to oversee the bank is not readily available or is not being provided to the board. The board needs to consider other situations that may indicate less than optimal oversight by management. The board should also consider whether the information is presented in such a manner that would readily allow the board to complete its mission.

Examples of red flags that generally apply to all areas covered in the Director's Reference Guide:

- The risk culture does not encourage employees to report improper activities or conduct.
- Risk management for individual risk areas or lines of business is not integrated into the bank's risk governance framework.
- Directors do not receive sufficient information to provide appropriate oversight over a given area.
- The bank's technology is no longer suitable for the bank's size, risk profile, operations, or strategic objectives, including new activities.
- The bank has an insufficient program to select and oversee third parties, including affiliates that provide products or services to the bank.
- The bank lacks adequate insurance coverage.
- The control environment has weaknesses.[11] Examples of red flags of potential control environment weaknesses include:
  - The bank does not have adequate and up-to-date policies in place for a given area.
  - There are adverse findings from IRM review, internal or external audit, or regulators, particularly when findings are increasing, repeated, or not corrected in a timely manner.
  - There is no or inadequate audit coverage of the area.
  - The external auditor's report expresses a qualified opinion, adverse opinion, or disclaimer of opinion.
  - The bank lacks clear lines of authority and accountability.
  - There is dominant influence from individual owners, managers, or directors.

[11] The control environment reflects the board's and management's commitment to internal controls. Internal control weaknesses can occur in all areas. Refer to the "Internal Controls" section of this guide for more information.

  - There is an increase in the volume of personnel failing to adhere to bank policies and procedures.
- Management is reluctant to provide information to the board, auditors, or regulators.
- The bank is not complying with laws or regulations, particularly if there is an increase in the volume or severity of violations of laws or regulations.
- The bank lacks an effective whistleblower process.
- There are whistleblower complaints.
- The bank is not conforming with strategies, plans, or risk limits, and there are no plans to bring operations into conformance.
- Personnel responsible for a given area lack the expertise, training, or resources needed.
- The bank does not have an adequate enterprise-wide complaint resolution process with adequate and timely tracking, monitoring, and resolution of complaints.
- The volume of complaints is significant or has increased, and the reports do not adequately address whether complaint trends or patterns increase risk, including risk of customer harm; reports do not adequately address remediation efforts.
- Some transactions with affiliates may not be in the bank's best interest.
- Management is unable to explain or provide support for assumptions used in models, particularly if the assumptions are supplied by a third party.

Strategic Planning

Sound strategic planning is essential for a bank to be competitive and profitable. The board is responsible for establishing the bank's strategic focus and significant long-term goals and for overseeing that the bank has the resources necessary to meet personnel, financial, technological, and organizational demands to execute the strategic plan. Planning should result in a board-approved, written strategic plan. The board should provide a credible challenge to management's assumptions and recommendations in the strategic plan. The board should oversee management's implementation of the strategic plan. With the help of progress reports, the board should carefully monitor and assess the strategic plan.

Key considerations in the bank's strategic planning process are growth, new profit opportunities, and responsible innovation[12] for the bank. These profit opportunities may include entering into strategic partnerships and expanding or introducing new products and services. 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. The board should require management to have a contingency plan if the original plan fails to achieve its objectives.

[12] The OCC defines "responsible innovation" as the use of new or improved financial products, services, and processes to meet the evolving needs of consumers, businesses, and communities in a manner that is consistent with sound risk management and that is aligned with the bank's overall business strategy.

Sources of Information

Examples of sources of information that directors review to oversee strategic planning:

- Strategic plan
- Risk appetite
- Capital plan
- Merger or acquisition plans
- Post-merger or acquisition analysis
- Change management reports
- Key initiative, project, or program updates
- Budgets and budget variance reports
- Budget assumptions
- Pricing and profitability reports
- New activities[13] reports
- Marketing plans
- Marketing data or reports
- Economic data or reports
- Staffing plans
- Talent management reports
- Income statement
- Balance sheet
- Litigation reports
- Insurance claims
- Information technology infrastructure reports
- IRM reports
- Audit reports
- Liquidity plans
- Asset/liability management reports

Measures

Examples of measures that directors review to oversee strategic planning:

- Budget variances
- Return on average assets (ROAA)
- Return on equity (ROE)
- Net interest margin (NIM)
- Noninterest income to average assets
- Overhead (non-interest expense) to average assets
- Efficiency ratio
- Cost of funds
- Yield on loans
- Yield on securities
- Equity growth versus asset growth
- Equity growth versus loan growth
- Gross off-balance-sheet items to total assets
- Depositor attrition
- Staffing attrition/retention

Questions to Consider

Examples of questions that directors may consider in their oversight of strategic planning:

- Does the strategic plan contain reasonable, realistic, and attainable goals and assumptions given the bank's circumstances?
- Is the strategic plan consistent with the risk appetite, capital plan, and liquidity requirements?
- If the plan is not executed as intended, fails, or objectives become unattainable, what mechanisms are in place to timely alert the board?
- Are the goals stated in the strategic plan clearly communicated or evident throughout the organization?
- Has management performed a retrospective review of merger or acquisition activity to compare actual outcome with planned outcome?

[13] New activities are defined in OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

- Are third parties performing as expected?
- What are the composition and quality of the bank's earnings?
- What are the most significant risks to earnings?
- What are the greatest challenges in maintaining or improving earnings?
- Has management taken on high-risk strategies to improve earnings? If so, what controls are in place to evaluate and manage the risks associated with such strategies?
- How do competitive pressures affect pricing for loans and deposits or management's ability to generate or maintain loans or deposits?
- What is the impact of nonrecurring or extraordinary gains or expenses on earnings performance?
- How is earnings performance being monitored?
- Is the budget periodically reviewed and updated?
- Are budget assumptions reasonable and compatible with the bank's risk appetite and strategic objectives?

Heightened Standards

- Does the strategic plan conform to the requirements outlined in heightened standards?[14]
- Does the strategic plan contain an explanation of how the covered bank will update, as necessary, the risk governance framework to account for changes in the risk profile projected under the strategic plan?[15]
- Is the strategic plan 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?[16]

Red Flags

Examples of red flags for directors regarding strategic planning:

- The bank does not have a board-approved, written strategic plan.
- The strategic plan does not include specific, measurable short- and long-term objectives.
- Management or the board do not fully understand the risks associated with success and failure of the strategic plan.
- There are no processes in place to monitor performance compared with the strategic plan.
- The bank's performance significantly varies from the bank's budgeted income statement and balance sheet or strategic plan.

[14] Refer to 12 CFR 30, appendix D.II.D, "Strategic Plan."

[15] Refer to 12 CFR 30, appendix D.II.D.3.

[16] Refer to 12 CFR 30, appendix D.II.D.4.

- Management does not adequately assess the resources, including staff, needed to meet the bank's goals and objectives or the potential impact of those goals and objectives on capital, earnings, and liquidity as well as any technology requirements and constraints.
- The strategic plan has not been revised in response to changes in the bank's condition or evidence of deteriorating economic conditions in markets or industries served by the bank.
- The bank pursues new activities or strategic partners without adequately assessing and analyzing the associated risks and rewards or without incorporating plans for new activities or strategic partners into the strategic planning process.
- Nonperforming assets and credit losses are inconsistent with economic data.
- The bank's risk profile has increased without a corresponding increase in capital or has exceeded the board's risk appetite.
  There are significant variances in key ratios, including ROAA, ROE, and NIM, from prior periods or peer group averages.
- The bank's income statement reflects earnings volatility.
- There is reliance on nonrecurring sources of income, such as extraordinary gains or favorable tax effects.
- Earnings performance is inconsistent with balance-sheet composition.
- There are significant increases or decreases in noninterest income or expenses.
- Management is unable or reluctant to identify and explain variances or trends in income, expense, or balance-sheet categories.
- Management is unable to adequately forecast or control funding and operating expenses.
- Expenses paid for services or salaries are excessive.
- Management is understaffed or is delaying capital improvements or other expenditures to enhance short-term profitability.
- Management is not properly reserving for or recognizing loan losses.

References

Examples of references that may assist directors in their oversight of strategic planning:

Regulations	• 12 CFR 5, "Rules, Policies, and Procedures for Corporate Activities" • 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 223, "Transactions Between Member Banks and Their Affiliates (Regulation W)"
Comptroller's Handbook	• "Analytical Review of Income and Expense" (national banks) • "Bank Supervision Process" • "Cash Accounts" (national banks) • "Community Bank Supervision" • "Corporate and Risk Governance" • "Large Bank Supervision" • "Litigation and Other Legal Matters" • "Recovery Planning" • "Related Organizations" (national banks)
Office of Thrift Supervision (OTS) Examination Handbook	• Section 730, "Related Organizations" (FSAs)
OCC bulletins	• 2010-24, "Incentive Compensation: Interagency Guidance on Sound Incentive Compensation Policies" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 2014-35: "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations" (mutual FSAs) • 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"

Capital Planning

Capital planning should align with a bank's strategic plan. Capital supports growth, fosters public confidence in the bank's condition, and is the cushion that protects banks, their customers, and shareholders against loss resulting from the assumption of risk. A bank is expected to maintain capital commensurate with the nature and extent of its risks as well as current and anticipated needs. Capital planning is a dynamic and ongoing process that, to be effective, should be forward looking in incorporating changes in a bank's strategic focus, risk tolerance levels, business plans, operating environment, or other factors that materially affect capital adequacy. Capital planning is especially critical for mutual FSAs, which are non-stock depository institutions, subject to the same regulatory capital requirements as stock banks. Unlike stock banks, mutual FSAs have very limited means to increase regulatory capital quickly and build capital almost exclusively through retained earnings.[17]

Stress testing is an essential element of the capital planning process as it enables the board to consider the impact to capital under various scenarios and helps management develop action plans to address negative outcomes.

Sources of Information

Examples of sources of information that directors review to oversee capital planning:

- Capital plan
- Strategic plan
- Liquidity plans
- Risk appetite
- Capital distribution or dividend policies
- Budgets and budget variance reports
- Stress testing reports
- Credit risk profile
- Fixed assets reports
- IRM reports
- Audit reports
- Income statement
- Balance sheet
- Concentration reports
- Asset/liability management reports

Measures

Examples of measures that directors review to oversee capital planning:

- Capital ratios
- Cash dividends to net income
- Equity growth versus asset growth
- ROE
- Equity growth versus loan growth
- Gross off-balance-sheet items to total assets
- Budget variances

[17] For more information, refer to OCC Bulletin 2014-35 and the "Capital and Dividends" booklet of the *Comptroller's Handbook*.

Questions to Consider

Examples of questions that directors may consider in their oversight of capital planning:

- What are the composition and quality of the bank's capital?
- What are the most significant risks to capital?
- How does the capital planning process assess capital adequacy in relation to the bank's overall risks and strategic direction?
- Does the capital plan include strategies for maintaining appropriate capital levels and identify contingent sources of capital?
- Is the capital planning process dynamic and forward-looking? Does it consider short- and long-term capital needs over at least three years?
- Are there impediments that could prevent the bank from accessing additional capital? If so, how does the capital plan account for these impediments?
- Has management explained how the stress testing process is in line with the bank's size, risk profile, and complexity? Are stress tests factored into the capital planning process?

Red Flags

Examples of red flags for directors regarding capital planning:

- The capital plan is not aligned with the strategic plan.
- Aggressive or rapid asset growth materially outpaces capital growth.
- Capital ratios are below minimums in the bank's capital plan, well-capitalized levels under 12 CFR 6, "Prompt Corrective Action," or minimums required by the OCC.
- Capital levels are not sufficient to support the bank's risk profile.
- Capital levels are well below peer group averages.
- There are significant fluctuations in capital ratios from quarter to quarter.
- Earnings are insufficient to augment capital or there is an overall declining earnings trend without a reasonable explanation.
- The bank is unable to or has only limited ability to raise capital, including no or limited access to capital markets or government assistance programs.
- Capital maintenance or growth depends on unusual or nonrecurring transactions or events.
- Dividend payouts are at the expense of adequately supporting operations, controls, or growth.[18]

[18] For more information, refer to 12 CFR 5, subpart E, "Payment of Dividends by National Banks" (national banks), and 12 CFR 5.55, "Capital Distributions by Federal Savings Associations" (FSAs).

- The bank's risk profile has increased without a corresponding increase in capital.
- There is a high level of nonperforming assets or interest rate risk (IRR) exposure relative to capital levels.
- Liquidity and funding sources are insufficient, or liquidity risk is high relative to capital levels.
- Stress tests do not have reasonable or supported assumptions, or results are adverse.

References

Examples of references that may assist directors in their oversight of capital planning:

Laws	• 12 USC 56, "Prohibition on Withdrawal of Capital; Unearned Dividends" (national banks) • 12 USC 59, "Reduction of Capital" (national banks) • 12 USC 60, "National Bank Dividends" (national banks)
Regulations	• 12 CFR 3, "Capital Adequacy Standards" • 12 CFR 5.55, "Capital Distributions by Federal Savings Associations" (FSAs) • 12 CFR 5, subpart E, "Payment of Dividends by National Banks" (national banks) • 12 CFR 6, "Prompt Corrective Action" • 12 CFR 46, "Annual Stress Test"
Comptroller's Handbook	• "Capital and Dividends"
Comptroller's Licensing Manual	• "Capital and Dividends"
OCC bulletins	• 2007-21, "Supervision of National Trust Banks: Revised Guidance: Capital and Liquidity" (trust banks) • 2012-14, "Interagency Stress Testing Guidance" • 2012-33, "Community Bank Stress Testing: Supervisory Guidance" • 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" • 2014-35: "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations" (mutual FSAs)

Earnings and Operational Planning

Operational plans, including budgets, marketing plans, staffing plans, and contingency plans, translate the long-term goals of the strategic plan into specific, measurable targets. The board should approve operational plans after concluding that plans are realistic and compatible with the bank's risk appetite and strategic objectives. Earnings should support operations and should provide for the maintenance of adequate capital and allowance for loan and lease losses (ALLL) or allowance for credit losses (ACL) levels. Earnings may be affected by (1) inadequately forecasted or controlled interest margins, sources of funding, or operating expenses; (2) improperly executed or ill-advised business strategies; or (3) poorly managed exposure to other risks.

Sources of Information

Examples of sources of information that directors review to oversee earning and operational planning:

- Strategic plan
- Risk appetite
- Budgets and budget variance reports
- Budget assumptions
- Pricing and profitability reports
- Marketing plans
- Marketing data or reports
- Staffing plans
- Talent management reports
- Income statement
- Balance sheet
- Nonrecurring income or expense items
- ALLL or ACL reports
- Liquidity plans
- Asset/liability management reports
- IRM reports
- Audit reports

Measures

Examples of measures that directors review to oversee earnings and operational planning:

- Staffing attrition/ retention
- Budget variances
- ROAA
- ROE
- Capital ratios
- NIM
- Noninterest income to average assets
- Overhead (non-interest expense) to average assets
- Efficiency ratio
- Earnings at risk
- Economic value of equity
- Cost of funds
- Yields on loans and investments
- Net losses to average total loans
- Past-due, nonaccrual, nonperforming, and charged-off loans and leases to total loans and leases
- Provision expense to average assets

Questions to Consider

Examples of questions that directors may consider in their oversight of earnings and operational planning:

- What are the composition and quality of the bank's earnings?
- What are the most significant risks to earnings?
- What are the greatest challenges in maintaining or improving earnings?
- Has management taken on high-risk strategies to improve earnings? If so, what controls are in place to evaluate and manage risks associated with those strategies?
- How do competitive pressures affect pricing for loans and deposits or management's ability to generate or maintain loans or deposits?
- What is the impact of nonrecurring income, such as extraordinary gains, or expenses on earnings performance?
- Is the budget periodically reviewed and updated?
- Are budget assumptions reasonable and compatible with the bank's risk appetite and strategic objectives?

Red Flags

Examples of red flags for directors regarding earnings and operational planning:

- There are significant fluctuations in performance ratios from quarter to quarter.
- Earnings are insufficient to augment capital, or there is a declining earnings trend.
- Nonperforming assets or credit losses are high or significantly increasing.
- IRR exposure relative to earnings or capital levels is high.
- There are significant variances in key ratios, including ROAA, ROE, and NIM, from prior periods or peer averages.
- Earnings are erratic, or the level or trend of earnings changes significantly.
- There are significant variances from budgeted amounts of income or expense items and balance-sheet accounts.

- There is reliance on nonrecurring sources of income, such as extraordinary gains or favorable tax effects.
- There are significant increases or decreases in noninterest income or expense.
- Complaint volumes or trends are high or increasing.
- Customer complaints indicate potential sales practices issues.
- Management is unable or reluctant to identify and explain variances or trends in income, expense, or balance-sheet categories.
- Budget assumptions do not align with the bank's risk appetite and strategic objectives or are unreasonable or unsupported.
- Management is unable to adequately forecast or control funding and operating expenses.
- Expenses paid for services or salaries are excessive.
- Management is understaffed or is delaying capital improvements or other expenditures to enhance or preserve short-term profitability.
- The percentage of nonperforming or classified loans to total loans is increasing at a greater rate than the ALLL or ACL balance.

References

Examples of references that may assist directors in their oversight of earnings and operational planning:

Comptroller's Handbook	• "Analytical Review of Income and Expense" (national banks) • "Bank Supervision Process" • "Capital and Dividends" • "Cash Accounts" (national banks) • "Community Bank Supervision" • "Corporate and Risk Governance" • "Large Bank Supervision"
Comptroller's Licensing Manual	• "Capital and Dividends"
OCC bulletins	• 2014-35: "Mutual Federal Savings Associations: Characteristics and Supervisory Considerations" (mutual FSAs) • 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles"

Risk Governance

Risk governance is the bank's approach to risk management. It applies the principles of sound corporate governance to the identification, measurement, monitoring, and controlling of risks to help ensure that risk-taking activities are in line with the bank's risk appetite and strategic objectives. Risk management includes the policies, processes, personnel, and control systems that support risk-related decision making. Risks should be assessed, evaluated, and managed enterprise-wide. Components of a risk governance framework include risk culture, risk appetite, and the bank's risk management system.

Sources of Information

Examples of sources of information that directors review to oversee risk governance:

- Risk appetite
- Risk assessments or risk assessment results
- IRM reports
- Concentration reports
- Audit reports
- Regulatory reports and communications
- Policy exception reports
- Issue status reports[19]
- Complaint reports
- Strategic plan and monitoring reports
- New activities reports
- Talent management reports
- Litigation reports
- Insurance coverage reports
- Compensation policies
- Benchmarking reports
- Senior management compensation reports
- Incentive compensation reports
- Organizational charts

Heightened Standards

Risk governance framework[20]

Risk appetite statement[21]

[19] Issue status reports can include items such as management self-identified issues, IRM review findings, internal audit findings, and regulatory findings.

[20] For more information, refer to 12 CFR 30, appendix D.II, "Standards for Risk Governance Framework."

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

Measures

Examples of measures that directors review to oversee risk governance:

- Risk appetite measures
- Early warning, key risk, and key performance indicators
- Concentration measures
- Issues status measures
- Complaint measures

Questions to Consider

Examples of questions that directors may consider in their oversight of risk governance:

- What are the bank's key risks in relation to the risk appetite and limits?
- Are limits expressed as a percentage of capital, as appropriate?
- What processes are in place for monitoring adherence to the risk appetite and risk limits?
- What are the processes when the bank is approaching risk limit(s)? What is the process for breached limit(s)? What is the process for remediating a breached limit?
- Are the scopes of risk assessments sufficient to identify material, emerging, and concentrations of risk?
- How are risk exposures aggregated to allow for identifying concentrations at the bank level, across lines of business, and between legal entities?
- What are the types, volumes, impacts, and trends of exceptions to policies and operating procedures?
- How is the risk culture coordinated throughout the bank? How are expectations conveyed to all employees?
- As the bank evolves in size, complexity, and operations, how does management determine whether the risk management system, internal controls, and the formality of the three lines of defense[22] remain appropriate and whether they are functioning as intended?
- Does the assessment of risk among the front line, IRM, and internal audit differ?
- How does management measure the effectiveness of its consumer complaint resolution process? Does the program track the identification and resolution of root causes?

[22] A common risk management system used in many banks, formally or informally, involves the three lines of defense model: (1) frontline units, business units, or functions that create and are responsible for risk; (2) IRM, which assess risk independent of the units that create risk; and (3) internal audit, which provides independent assurance to the board on the effectiveness of governance, risk management, and internal controls. Most banks have the basic elements of the three lines of defense model. For more information, refer to the "Corporate and Risk Governance" booklet of the Comptroller's Handbook.

- What are the results of the independent assessments of the risk governance framework? Does senior management appropriately update the framework to address findings?
- How does management identify changes to control systems needed, including quality control and quality assurance, for risk management to keep pace with changes in bank operations, activities, risk profile, and industry standards?

Heightened Standards

Does the risk governance framework conform to the requirements outlined in heightened standards?[23]

How do frontline units assess, on an ongoing basis, and appropriately manage the material risks associated with their activities?[24]

How does IRM assess, on an ongoing basis, the covered bank's material aggregate risks and communicate to the board or risk committee significant instances where IRM's risk assessment differs from a frontline unit's assessment?[25]

How does internal audit independently assess the design and ongoing effectiveness of the risk governance framework and has its most recent assessment concluded that the covered bank is in compliance with heightened standards?[26]

Does the comprehensive written risk appetite statement require review and approval more than annually 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?[27]

Red Flags

Examples of red flags for directors regarding risk governance:

- The board is not leading by example by setting a strong culture of compliance and holding management accountable.
- The chief risk executive or board-appointed person or committee to oversee enterprise risk management does not have the expertise, stature, or authority to be effective and does not have unfettered access to the board or risk committee to communicate risk concerns.

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

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

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

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

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

- The bank lacks clear lines of authority and accountability.
- Compensation arrangements, particularly incentive arrangements, do not reflect a reasonable balance between risk and reward and do not include measures to dissuade risk-taking outside of established tolerances.
- Employee incentives do not reward appropriate behavior or penalize inappropriate behavior.
- Management's actions are inconsistent with the stated and intended risk culture and established tolerances.
- Risks are not identified, measured, monitored, or controlled enterprise-wide.
- Management lacks the ability to aggregate risk exposures and identify concentrations timely and accurately at the bank level, across lines of business, or between legal entities.
- Strategic, operating, capital, liquidity, or other plans include inconsistent information or are incongruent.
- Reports about current and emerging risks and their potential impact on earnings, capital, or strategic objectives are neither transparent nor comprehensive.
- Reports do not address the bank's material risks and key controls in the context of the bank's risk appetite and limits.
- There is a lack of independent assessments of the risk governance framework or its components.
- Risk assessments are not performed on key banking activities or are performed without sufficient frequency.
- The bank lacks an effective process to identify, escalate, and address material risks and risk-taking activities that exceed the approved risk appetite and limits.
- There are continued risk limit breaches.
- Risk limits are unrealistic or inconsistent with the risk appetite.
- Management is unable or unwilling to self-identify issues, is failing to comply with policies, or is participating in unethical practices.
- A proper assessment of root causes and trends has not occurred for issues or litigation.
- Issue tracking and resolution processes are inadequate for identifying material implications for the bank's risk profile.
- Corrective actions to address issues are completed in an untimely manner or target dates are moved without justification.
- The number of issues identified by regulators, lines of business, IRM, compliance, or audit is high or increasing, or there are repeat issues. Such issues may include matters requiring attention, violations of laws and regulations, bank policy exceptions, control weaknesses, or complaints.

- The complaint resolution process is not in line with the bank's size, complexity, or operations.
- There are whistleblower complaints.

Heightened Standards

The covered bank is not adhering to, or is not working toward adherence to, the requirements outlined in heightened standards for the risk governance framework's design and implementation.[28]

References

Examples of references that may assist directors in their oversight of risk governance:

Regulations	• 12 CFR 30, "Safety and Soundness Standards"
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Compliance Management Systems" • "Corporate and Risk Governance" • "Internal and External Audits" • "Large Bank Supervision"
OCC bulletins	• 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies" • 2019-37, "Operational Risk: Fraud Risk Management Principles"
Other	• Basel Committee on Banking Supervision – "Principles for Effective Risk Data Aggregation and Risk Reporting," January 2013 – "Corporate Governance Principles for Banks," July 2015

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

Internal Controls

An effective system of internal controls is the foundation of sound risk management. It should be properly designed and consistently enforced. The system of internal controls includes the systems, policies, procedures, and processes effected by the board, management, and other personnel that are designed to limit or control risk, achieve the bank's objectives, and safeguard bank assets and information, and effectuate compliance with laws and regulations. Effective internal controls support sound corporate and risk governance and reduce the potential for mismanagement, operational losses, significant errors, irregularities, and fraud, and assist with timely detection of such issues when they occur. A commitment by the board and senior management is fundamental to a sound system of internal controls. Audit, when properly structured and conducted, provides an objective, independent assessment of the quality of the bank's internal controls.

Sources of Information

Examples of sources of information that directors review to oversee internal controls:

- Audit reports
- IRM reports
- Management internal control attestations
- Control and risk assessments (e.g., risk and control self-assessments [RCSA])
- Operational loss reports
- Security incident reports
- Policy exception reports
- Issue status reports
- Quality assurance reports
- Quality control reports
- Regulatory reports and communications
- Change management reports
- New activities reports
- Training reports
- Fraud reports
- Litigation reports
- Whistleblower complaint reports
- Complaint reports
- Employee exit interview reports

Measures

Examples of measures that directors review to oversee internal controls:

- Financial reporting error rates
- Complaint measures
- Measures that report on the effectiveness of the internal control environment
- Measures on the use of automated versus manual controls
- Violation measures
- Issues status measures
- Policy exception rates
- Operational loss measures
- Fraud measures

Questions to Consider

Examples of questions that directors may consider in their oversight of internal controls:

- How does management demonstrate its commitment to maintaining a sound control environment across the bank?
- How does management communicate the control culture so all employees understand their responsibility for internal controls and so employees understand their responsibility to report circumvention of controls?
- How does management ensure that the relevant lines of business, IRM, and audit personnel participate in the risk assessment process?
- What ongoing assessments (such as self-assessments and testing) of internal controls do business units and IRM conduct?
- What are the results of the testing of the effectiveness of the internal controls? Does management effectively report on the results to identify root causes and themes?
- How are risks and controls evaluated to facilitate strategic planning and approval of strategic objectives (such as those related to new activities, change management, systems, or third-party relationships)?
- How are internal controls monitored enterprise-wide?
- Does management enforce a vacation policy for employees in sensitive positions to be absent for a least a consecutive two-week period?
- Is audit coverage adequate?
- What is the process for confirming that effective corrective actions of material control weaknesses are monitored and implemented on a timely basis?
- Who reviews the actions that management takes to address material control weaknesses?
- How is management held accountable if it does not satisfactorily remediate significant control weaknesses in a timely manner?
- What is management's or auditors' assessment of the effectiveness of internal controls and procedures for financial reporting?[29]
- What, if any, potential matters could affect management's annual assessment of the bank's internal controls and, if applicable, the external auditor's attestation of management's assertions?[30]

[29] 12 CFR 363.3(b), "Internal Control Over Financial Reporting," requires independent public accountants of an insured depository institution with total assets of $1 billion or more to examine, attest to, and report separately on the assertion of management.

[30] Ibid.

Red Flags

Examples of red flags for directors regarding internal controls:

- There is an absence or failure of key structures for a sound control environment or in key control activities, such as segregation of duties, dual controls, rotation of duties, approvals, verifications, reconciliations, and reviews of operating performance.
- Employees generally do not identify or report deficiencies or breaches in internal controls.
- The bank's operations, activities, or risk profile has changed, but internal controls have remained the same.
- Staff is inadequately trained on internal policies, procedures, and controls.
- Operational losses are high or increasing.
- Security breaches have resulted in unauthorized access to or use of customer or bank information.
- Business units do not complete risk self-assessments or testing with sufficient frequency.
- Identified internal control deficiencies, IRM findings, audit findings, or regulatory findings are not corrected in a timely manner, or there are repeat findings.
- A proper assessment of root causes and trends has not occurred for significant control deficiencies, complaints, or litigation.
- The audit function lacks independence.
- Management does not provide sufficient reporting on the overall effectiveness of the internal control environment and root causes for significant areas of weaknesses.
- Management does not provide timely and accurate financial, operational, and regulatory reports.
- Reports do not provide sufficient detail to understand primary control functions, key risks, and emerging risks.
- External auditors provide a qualified, adverse, or disclaimer opinion.

References

Examples of references that may assist directors in their oversight of internal controls:

Laws	• Pub. L. 107-204, 116 Stat. 745 (2002), Sarbanes–Oxley Act of 2002
Regulations	• 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 162, "Accounting and Disclosure Standards" (FSAs) • 12 CFR 363, "Annual Independent Audits and Reporting Requirements"
Comptroller's Handbook	• "Corporate and Risk Governance" • "Internal and External Audits" • "Internal Control" (national banks)
OTS Examination Handbook	• Section 340, "Internal Control" (FSAs)
OCC bulletins	• 1999-37, "Interagency Policy Statement on External Auditing Programs" • 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing" • 2016-2, "Interagency Advisory on External Audits of Internationally Active U.S. Financial Institutions"
Other	• Basel Committee on Banking Supervision – "Framework for Internal Control Systems in Banking Organisations," September 1998 – "The Internal Audit Function in Banks," June 2012 – "External Audits of Banks," March 2014 • Committee of Sponsoring Organizations of the Treadway Commission – "Internal Control—Integrated Framework," May 2013

Operational Risk

Operational risk is the risk to the bank's current and projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events. Operational risk is present in all aspects of bank activities and can expose the bank to material losses. All banks, regardless of size, should have policies, processes, personnel, and control systems sufficient to manage the bank's operational risk.

Sources of Information

Examples of sources of information that directors review to oversee operational risk:

- Operational risk management framework
- Operational risk profile
- Operational risk assessments
- Operational risk appetite
- Stress testing reports and results
- Operational loss reports
- Scenario analysis
- Security incident reports
- Quantitative decision-making tools
- Operational risk taxonomy (e.g., defined terms and operational event types)
- Issue status reports
- Key initiative, project, or program updates
- New activities reports
- Insurance coverage reports
- Business continuity and disaster recovery plans and testing results
- Third-party risk management reports
- Fraud reports
- Litigation reports
- Complaint reports
- IRM reports
- Audit reports

Measures

Examples of measures that directors review to oversee operational risk:

- Operational loss measures
- Employee turnover measures
- Project budget variance reports
- Transaction processing error rates
- Reconciliation discrepancy measures
- Fraud measures
- Complaint measures
- Litigation measures
- Issues status measures

Questions to Consider

Examples of questions that directors may consider in their oversight of operational risk:

- What is the bank's operational risk profile?
- What are the bank's top operational risks?

- How does the bank manage operational risk? Is it centralized or decentralized? Is it in line with the bank's size, complexity, and risk profile? For larger, more complex banks, is the IRM function objectively identifying, measuring, monitoring, and reporting operational risk on an enterprise basis?
- What risk management tools are used to manage operational risk?
- What processes are in place to collect, aggregate, and analyze operational risk data in specific areas across lines of business on an enterprise-wide basis to assist in identifying similar events or patterns occurring in more than one area?
- How are policies, roles, responsibilities, and accountability for operational risk communicated and implemented bank-wide?
- What processes are in place to verify conformance with operational-related policies and risk limits?
- How does management investigate and report on the root causes of actual or potential operational loss events, gains, and near misses?
- What is the process for completing risk assessments (e.g. RCSAs)? Does management appropriately track and monitor resulting action plans to confirm that necessary actions are properly implemented?
- What is the bank's level of success in preventing operational failures? What is being done to improve these levels?
- How does bank management use industry or external operational loss trends?
- To what extent are operational risk assessment activities integrated into the bank's strategic planning processes (such as processes related to new activities and change management)?
- How does bank management respond to increasing operational risk resulting from new activities, processes, delivery challenges, or third-party relationships?
- How might the operational risk exposure be affected by changes in strategic or operational plans? Does management consider the cost and benefits' impact on strategic or operating plans when determining risk management strategies?
- Does the bank allocate sufficient financial and personnel resources to properly identify, measure, monitor, and control operational risks?
- How are KRIs and KPIs determined? Do they address all key operational risks within the bank?
- What escalation processes and reporting thresholds have been established for material operational risk events, near misses, cumulative patterns, or breaches?

Red Flags

Examples of red flags for directors regarding operational risk:

- Management is unable to determine the bank's operational risk exposure.
- Exposure to risk from errors or processing disruptions is significant given the volume of transactions, complexity of activities, or state of internal systems.
- Operational losses are high or increasing.
- Fraud losses are high or increasing.
- Management does not have processes in place to recognize enterprise wide operational issues or patterns. Management has not established action plans for high-risk events.
- For larger, more complex banks, there is an inconsistent taxonomy of operational risk terms (e.g., the definition of operational risk and operational risk event types) used throughout the bank.
- The bank lacks a risk assessment (e.g., RCSA) process to assess inherent operational risks or the design and effectiveness of associated controls.
- There are deficiencies in third-party risk management, particularly if the number of outsourced services for critical activities is high.
- Business continuity management focuses solely on recovery of information technology capabilities and does not include the recovery and resumption of all aspects of the bank's business processes, including operations supported by third parties.[31]
- Complaint volumes or trends are high or increasing.
- The number of attempted cyberattacks against bank systems is increasing.

References

Examples of references that may assist directors in their oversight of operational risk:

Regulation	• 12 CFR 3, subpart E, "Risk-Weighted Assets—Internal Ratings-Based and Advanced Measurement Approaches" • 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 46, "Annual Stress Test"
Comptroller's Handbook	• "Corporate and Risk Governance" • "Internal Control" (national banks)

[31] Refer to the "Information Technology" section of this guide for more information on business continuity management.

Regulation	• 12 CFR 3, subpart E, "Risk-Weighted Assets—Internal Ratings-Based and Advanced Measurement Approaches" • 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 46, "Annual Stress Test"
OTS Examination Handbook	• Section 340, "Internal Control" (FSAs)
OCC bulletins	• 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies" • 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" • 2011-21, "Interagency Guidance on Advanced Measurement Approaches for Operational Risk" • 2012-14, "Interagency Stress Testing Guidance" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 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" • 2017-7, "Third-Party Relationships: Supplemental Examination Procedures" • 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles" • 2018-8, "FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs" • 2019-37, "Operational Risk: Fraud Risk Management Principles" • 2020-5, "Cybersecurity: Joint Statement on Heightened Cybersecurity Risk" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
Other	• Basel Committee on Banking Supervision – "Principles for Effective Risk Data Aggregation and Risk Reporting," January 2013 – "Review of the Principles for the Sound Management of Operational Risk," October 2014 • *Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook*

Information Technology

Information technology (IT) vulnerabilities can arise from internal and external factors, including cybersecurity and data security threats and rapidly evolving technology and products. Information technology risk management involves back-office operations, payment systems, network administration, systems development and acquisition, business continuity management, information security, cyber security, data governance, and third-party risk management. Further, the Gramm–Leach–Bliley Act requires the board to approve and oversee the development, implementation, and maintenance of the bank's information security program.[32]

Sources of Information

Examples of sources of information that directors review to oversee IT:

- Information technology policies
- Information security policies
- Cybersecurity policies
- Risk assessments (e.g., security, resilience, continuity)
- Business impact analysis
- Business continuity and disaster recovery plans and testing results
- Phishing test results
- Key initiative, project, or program updates
- New activities reports
- End-of-life system reports
- Threat landscape summary
- Incident response plan
- Security incident reports
- Unplanned technology outage reports
- Verification of employee access levels
- Inventory of critical third-party relationships, including IT service providers
- Third-party risk management reports
- Gramm–Leach–Bliley Act report to the board
- Penetration testing and vulnerability assessment results
- Status of vulnerability and maintenance patching programs
- Issues status reports
- Training reports
- Audit reports

Measures

Examples of measures that directors review to oversee IT:

- Performance that has breached thresholds in service-level agreements
- Overall system availability
- Overall platform availability
- Overall application availability
- End-of-life system measures
- Production incidents
- Resource costs
- Issues status measures

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

Questions to Consider

Examples of questions that directors may consider in their oversight of IT:

- How do the products and services offered—and delivery channels, technologies, and connection types used—collectively affect the bank's overall risks, including cybersecurity risk?
- How does management leverage threat and vulnerability information to improve risk management practices?
- How are the business continuity and disaster recovery plans validated? Is there comprehensive testing? Does testing include third parties?
- What processes are in place to confirm compliance with the Gramm–Leach–Bliley Act?
- Does the information security program adequately include administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information?
- How are information security responsibilities and accountability defined and communicated throughout the bank?
- What training do employees receive on information security and cybersecurity?
- What is the bank's plan if breaches occur? Is there a well-established and tested response plan in place that clearly designates appropriate personnel for key response mechanisms?
- Are sufficient resources allocated to IT risk management? Do individuals, such as the chief information officer, chief information security officer, chief operating officer, or chief technology officer, provide the board with periodic updates on the bank's information technology infrastructure, operations, and information security-related risks?
- How does management make available appropriate cybersecurity awareness materials to employees and customers?
- What is the bank's maturity level based on results from the FFIEC's Cybersecurity Assessment Tool? What controls should or could be added to increase maturity?
- How does management proactively manage end-of-life systems? What end-of-life systems does the bank have and what are management's plans regarding these systems?
- How often are data and systems backed up, including information housed at third parties?
- What controls are in place to confirm the integrity of backed-up data?
- How does management ensure the bank's IT systems are appropriate to support new activities?
- What is the bank's process for complying with breach notification laws in the jurisdictions where the bank operates?

Red Flags

Examples of red flags for directors regarding IT:

- Business continuity management focuses solely on recovery of information technology capabilities and does not include the recovery and resumption of all aspects of the bank's business processes, including operations supported by third parties.
- A business impact analysis, as part of business continuity management, has not been documented for each business process and supporting technology system.
- Disaster recovery plans include unrealistic time frames for recovering and restoring data and applications.
- The disaster recovery plans and business continuity plans have not been tested thoroughly or frequently enough to provide adequate assurance of the bank's ability to resume operations in a timely manner.
- Disaster recovery and business continuity testing show adverse results.
- The information security risk assessment does not consider or include control testing results, including information technology audit, vulnerability assessments, or penetration testing.
- There is inadequate testing of key controls, including penetration tests, testing of changes to systems or processes, or vulnerability assessments.
- There is an excessive number of employees with system access beyond what is needed for their job responsibilities.
- The number and impact of breaches is high or significantly increasing.
- The bank lacks policies that direct how to handle damages or liability resulting from data loss or theft.
- Authentication controls are weak.
- The incident response plan and accompanying procedures are not well communicated throughout the bank.
- Incident responses are untimely.
- The incident response plan is not appropriately tested.
- Employees are consistently failing phishing tests.
- The bank or its service providers use unpatched or unsupported software or hardware.
- The bank does not maintain a comprehensive inventory of hardware, operating systems, and application software, including end-of-life support dates.
- Systems and data are not backed up on a frequency commensurate with the risk and complexity of the technology environment.
- An insufficient number of iterations of backups are maintained.
- The number of attempted cyberattacks against bank systems is increasing.

References

Examples of references that may assist directors in their oversight of IT:

Regulations	• 12 CFR 7, subpart E, "National Bank Electronic Activities" (national banks) • 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards" • 12 CFR 155, "Electronic Operations of Federal Savings Associations" (FSAs)
Comptroller's Handbook	• "Community Bank Supervision" • "Corporate and Risk Governance" • "Large Bank Supervision" • "Merchant Processing" • "Payment Systems and Funds Transfer Activities" (national banks)
OTS Examination Handbook	• Section 580, "Payments Systems Risk" (FSAs)
OCC bulletins	• 2003-14, "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System: Business Continuity Sound Practices Developed by the FRB, SEC, and OCC to Ensure the Continued Functioning of Critical Financial Services" (national banks) • 2005-13, "Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance: Interagency Guidance" • 2005-24, "Fraudulent Bank Websites: Risk Mitigation and Response Guidance for Website Spoofing Incidents" • 2005-44, "Small Entity Compliance Guide: Information Security" • 2008-16, "Information Security: Application Security" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 2016-34, "Cybersecurity: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool" • 2017-7, "Third-Party Relationships: Supplemental Examination Procedures" • 2020-5, "Cybersecurity: Joint Statement on Heightened Cybersecurity Risk" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
Other	• *FFIEC Information Technology Examination Handbook* • National Institute of Standards and Technology's Cybersecurity Framework • U.S. Department of Homeland Security's *National Cyber Incident Response Plan*, December 2016

Third-Party Risk Management

A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.[33] The bank should have effective risk management regardless of whether the bank performs an activity internally or through a third party. 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.[34]

Sources of Information

Examples of sources of information that directors review to oversee third-party risk management:

- Third-party risk management reports
- Third-party risk management policies
- Inventory of critical third-party relationships, including information technology service providers
- Third-party concentration risk reports
- Summaries of due diligence of third parties involved in critical activities
- Reports of third parties not meeting service-level agreements
- Analyses of costs associated with third-party relationships
- Third-party-related budget variance reports
- Complaint reports
- Contracts with third parties involved in critical activities
- Contingency plans for third-party relationships involving critical activities
- Business continuity and disaster recovery plans and test results
- Reports of examination of service providers
- IRM reports
- Audit reports

[33] Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records.

[34] A bank that enters into a third-party relationship with another OCC-supervised bank is expected to implement the same standards of due diligence, controls, and oversight as with any other third party.

Measures

Examples of measures that directors review to oversee third-party risk management:

- Percentage of third-party relationships involving critical activities
- Percentage of ongoing monitoring reviews that are past due
- Service-level agreement measures
- Percentage of third-party relationships with missing ongoing monitoring documentation
- Third-party-related budget variances
- Complaint measures

Questions to Consider

Examples of questions that directors may consider in their oversight of third-party risk management:

- Does the bank have a comprehensive process for assessing risks relating to the use of third parties?
- How does management assess the level of risk and complexity of each third-party relationship? Is the risk management of each third-party relationship commensurate with the level of risk and complexity?
- How does management confirm the completeness of the inventory of third-party relationships?
- Who is responsible for reviewing and approving contracts? Has management established criteria for when a contract should be reviewed by legal counsel?
- What controls are in place to prevent employees from engaging a third party without undertaking the proper approval process?
- Does management's assessment of third-party relationships identify third parties with access to customers' personally identifiable information?
- Who is responsible for reviewing technical information for initial due diligence and ongoing monitoring? Are they subject matter experts?
- What are the ongoing monitoring requirements for third parties? Is the information sufficient to determine whether to continue the relationship? How is the timely completion of reviews tracked?
- How does management include third parties in business continuity tests?
- How does management confirm appropriate access for third parties and subcontractors to the bank's information assets?
- How does management monitor complaints received by or about third parties?
- What are the costs associated with each activity or third-party relationship? Are there indirect costs assumed by the bank?

Red Flags

Examples of red flags for directors regarding third-party risk management:

- Management does not maintain an effective third-party risk management process that follows a continuous life cycle for all relationships, including planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination.
- The inventory of third-party relationships is not comprehensive.[35]
- Management has not determined the level of risk of all of the bank's third parties.
- Management does not determine if the bank's third parties use subcontractors.
- The bank does not have information about the complaints that the bank's third parties receive.
- Complaints regarding activities with significant third-party involvement are high or increasing.
- Management has not identified which of the bank's third parties have access to the bank's customers' personally identifiable information—both physical and virtual.
- Contracts do not have provisions that (1) require notice of information security breaches that occur at the third party or by subcontractors; (2) address third parties that fail to perform proper due diligence on subcontractors (e.g., fourth party); and (3) address requirements for the fourth party (e.g., for information security, disaster recovery, etc.).
- The number of past due ongoing monitoring reviews is high or increasing.
- The number of third parties not meeting service level agreements is high or increasing.
- There is a significant amount of missing ongoing monitoring documentation.
- Management does not present the results of due diligence to the board when making recommendations for third-party relationships involving critical activities.
- Management does not take appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring of third parties.
- The board does not approve the contracts for third-party relationships providing critical activities.

[35] The most common relationships missing from an inventory of third-party relationships include affiliates and subsidiaries; relationships with other banks; utilities; the Board of Governors of the Federal Reserve System, government-sponsored entities, or the Depository Trust Company; joint ventures or strategic partnerships; entities that support the human resource function; or attorneys, appraisers, or consultants.

- The board does not receive periodic reports on the status and results of ongoing monitoring reviews for third parties providing critical services.
- The bank's contingency plans do not address critical third parties.

References

Examples of references that may assist directors in their oversight of third-party risk management:

Comptroller's Handbook	• "Compliance Management Systems" • "Corporate and Risk Governance" • "Internal and External Audits"
OCC bulletins	• 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 2017-7, "Third-Party Relationships: Supplemental Examination Procedures" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
Other	• *FFIEC Information Technology Examination Handbook* – "Business Continuity Management" – "Outsourcing Technology Services" – "Supervision of Technology Service Providers"

Fraud Risk Management

Potential exposure to internal and external fraud exists in all bank activities. Fraud can involve employees, insiders, customers, and external parties, including third parties engaged by the bank. Fraud continuously evolves, presenting challenges for identifying and implementing effective controls. While not all fraud can be avoided completely, active directors foster an environment in which fraud is more likely to be prevented, deterred, and promptly detected through appropriate fraud risk management.

Sources of Information

Examples of sources of information that directors review to oversee fraud risk management:

- Fraud risk profile
- Fraud risk assessment
- Fraud loss reports
- Code of ethics
- Insider activities policies
- Compensation policies
- Budget variance reports
- Security incident reports
- Whistleblower complaint reports
- Employee exit interview reports
- Information on suspicious activity reports (SAR) regarding fraud or insider abuse
- Complaint reports
- Litigation reports
- Insurance coverage reports
- Fraud investigation reports
- IRM reports
- Training reports
- Audit reports

Measures

Examples of measures that directors review to oversee fraud risk management:

- Measures by fraud type (e.g., internal, external, loan, card, account opening, check, or embezzlement)
- Fraud loss measures (e.g., per open account, closed account, or litigation)
- Fraud recoveries
- Insurance claim measures
- Litigation measures
- Budget variances
- Automated clearing house (ACH) return rates
- Percentage of customers claiming victim fraud
- Fraud investigation measures
- Complaint measures
- Bank Secrecy Act (BSA) report measures
- Civil and criminal subpoena

Questions to Consider

Examples of questions that directors may consider in their oversight of fraud risk management:

- Do bank policies, processes, and control systems indicate a strong stance against fraud and promote appropriate and timely investigations into, responses to, and reporting[36] of suspected and confirmed fraud?
- When fraud has occurred, what changes have been implemented to prevent a reoccurrence?
- How are the bank's internal controls and fraud risk management assessed for effectiveness?
- How effective is the bank's internal control environment? Does the bank adequately use and review internal controls (e.g., segregation of duties and dual controls)? Has audit identified weaknesses? What is the root cause for those weaknesses and are they being corrected in a timely, appropriate, and sustainable manner?
- What type of fraud risk management training and awareness do employees and contractors receive and does the training and awareness campaign address how to prevent, identify, and report fraud?
- How often is a fraud risk assessment completed? How are information security and cybersecurity reflected in the fraud risk assessment?
- What is the process of assessing the impact to the bank's fraud risk profile as new activities are being considered?
- What is the bank's process for analyzing and resolving complaints?

Red Flags

Examples of red flags for directors regarding fraud risk management:

- The bank's risk management system does not include fraud risk management principles commensurate with the bank's size, complexity, and risk profile to effectively prevent, detect, and respond to fraud.
- Management does not perform an adequate fraud risk assessment.
- The board does not receive sufficient information regarding the amount and types of fraud.
- Fraudulent activity is high or is significantly increasing.
- Identified fraud is not appropriately or timely investigated to determine why it occurred or if it could occur in other areas.

[36] Reporting should allow management and directors to measure performance. Additionally, a bank is required to file an SAR for known or suspected fraud meeting regulatory thresholds. Refer to 12 CFR 21.11, "Suspicious Activity Report" (national banks), and 12 CFR 163.180, "Suspicious Activity Reports and Other Reports and Statements" (FSAs).

- When significant fraud has occurred, management did not implement changes to prevent a reoccurrence.
- Information technology practices do not include user access reviews, or the bank has inadequate information security practices.
- There are frequent changes in auditors.
- The bank does not provide training to employees on fraud or does not have fraud awareness campaigns.
- Hiring practices allow hiring employees in key or high-risk positions without adequate due diligence or background investigations.
- The bank lacks adequate insider activities policies.
- There is no policy requiring officers and employees to be away from their duties for an uninterrupted period of not less than two consecutive weeks (e.g., vacation or rotation of duties). Alternatively, there is such a policy, but it is not enforced.
- Insider transactions are not appropriately monitored.
- Compensation does not appropriately balance risk and reward to prevent incentives that expose the bank to imprudent risk and to prevent incentives for employees to engage in unethical business development.
- The number of attempted cyberattacks against bank systems is increasing.

References

Examples of references that may assist directors in their oversight of fraud risk management:

Regulations	• 12 CFR 21, subpart A, "Minimum Security Devices and Procedures" (national banks) • 12 CFR 41, subpart J, "Identity Theft Red Flags" • 12 CFR 168, "Security Procedures" (FSAs)
Comptroller's Handbook	• "Compliance Management Systems" • "Corporate and Risk Governance" • "Internal and External Audits" • "Internal Control" (national banks)
OTS Examination Handbook	• Section 340, "Internal Control" (FSAs) • Section 360, "Fraud and Insider Abuse" (FSAs)

Regulations	• 12 CFR 21, subpart A, "Minimum Security Devices and Procedures" (national banks) • 12 CFR 41, subpart J, "Identity Theft Red Flags" • 12 CFR 168, "Security Procedures" (FSAs)
OCC bulletins	• 2005-24, "Fraudulent Bank Websites: Risk Mitigation and Response Guidance for Website Spoofing Incidents" • 2007-2, "Fraudulent Cashier's Checks: Guidance to National Banks Concerning Schemes Involving Fraudulent Cashier's Checks" (national banks)[37] • 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 2017-7, "Third-Party Relationships: Supplemental Examination Procedures" • 2019-37, "Operational Risk: Fraud Risk Management Principles" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
Other	• Committee of Sponsoring Organizations of the Treadway Commission and Association of Certified Fraud Examiners: – "Fraud Risk Management Guide" and "Executive Summary," September 2016 • FFIEC Publications – "The Detection, Investigation and Prevention of Insider Loan Fraud: A White Paper," May 2003 – "The Detection, Investigation, and Deterrence of Mortgage Loan Fraud Involving Third Parties: A White Paper," February 2005 – "The Detection and Deterrence of Mortgage Fraud Against Financial Institutions: A White Paper," February 2010

[37] Although OCC Bulletin 2007-2 applies to national banks, directors of FSAs may find the information useful.

As of March 2025, references to reputation risk have been removed from this publication. Refer to OCC Bulletin 2025-4.

Payment Systems

Payment system risk includes potential loss or harm associated with sending or receiving payments or information about payments. The risks can be connected to payment and settlement activity, as well as clearing, transmitting, and recording transactions, and could have an adverse effect on a bank's earnings and capital. The risks generally associated with payment systems include operational, compliance, strategic, credit, and liquidity, but all risk types may be affected. Risk management practices for payment systems should directly correspond with the specific payment products and services offered, and the complexity and risk of those offerings. Appropriate risk management includes identifying, measuring, monitoring, and controlling payment system risk commensurate with the bank's risk appetite and strategic objectives.

Sources of Information

Examples of sources of information that directors review to oversee payment systems:

- Descriptions of payment products, services, or channels offered and used by the bank
- Payment-related policies (e.g. lending policies, liquidity policies)
- Payment settlement reports
- Inventory of critical third-party relationships,[38] including information technology service providers
- Reports of third parties not meeting service-level agreements
- Operational loss reports
- Fraud loss reports
- Charge-back reports
- ACH activity reports
- Issues status reports
- Complaint reports
- Control and risk assessments (e.g., RCSA)
- Business continuity and disaster recovery plans and testing results
- Payment system incident reports
- Litigation reports
- Audit reports
- Policy exception reports
- Training reports

[38] Payments-related third-party relationships may include payment processors, ACH service providers, merchant (card) processors, remote deposit capture service providers, holding companies and affiliates, correspondent banks, affinity card program managers, automated teller machine providers, lock box service providers, and third-party senders.

Measures

Examples of measures that directors review to oversee payment systems:

- Charge-back volumes and trends
- Return rates by originator and, as applicable, third-party senders
- ACH activity volume
- Payment-related service-level agreement measures
- Operational loss measures
- Fraud loss measures
- Transaction volume variances from previous periods
- Complaint analysis
- Issues status measures

Questions to Consider

Examples of questions that directors may consider in their oversight of payment systems:

- How does management measure and monitor credit exposure from ACH debits?
- How does management incorporate credit exposure resulting from payment activities into credit monitoring?
- How are payment, clearing, and settlement activities included in liquidity risk management practices?
- How are payment systems incorporated into business continuity and disaster recovery plans?
- What are the bank's risk exposures from its financial market infrastructures[39] memberships?
- If the bank offers ACH processing, what processes are in place to maintain compliance with National Automated Clearing House Association (NACHA) Operating Rules and Guidelines?[40]
- How do payment functions or units coordinate anti-fraud policies, procedures, and practices?
- How do payment personnel monitor for suspicious payment activities and potentially fraudulent activities?
- How are payment system audits and reviews performed—on a firm-wide basis or on a line-of-business basis? Are the reviews appropriate for the nature and extent of the bank's payment activities? How does audit identify systemic issues across multiple products, services, and delivery platforms?

[39] The Bank for International Settlements defines financial market infrastructures as a multilateral system among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

[40] Refer to the "Retail Payment Systems" booklet of the *FFIEC Information Technology Examination Handbook* for more information. (Note: Although the OCC does not enforce NACHA Operating Rules and Guidelines, nonconformance can result in safety and soundness concerns and subjects the bank to NACHA's ACH Rules Enforcement and potential monetary fines.)

Red Flags

Examples of red flags for directors regarding payment systems:

- The strategic plan does not address the products and services offered, delivery channels used, and technologies implemented in the bank's payment systems.
- Credit policies do not include underwriting standards for ACH originators, commercial remote deposit capture customers, and other applicable payment customers.
- Reports on payment system incidents do not contain analysis of duration, customer impact, and related losses.
- The aggregate exposure of overdraft lines is not analyzed.
- The third-party relationship inventory does not include payment-related third-parties.
- The scope or frequency of compliance monitoring is not commensurate with the nature of payment activities and the overall risk profile.
- The bank's system of internal controls is inadequate given the level of complexity of the payment products, services, and delivery channels.
- Employees in payment-related areas do not receive appropriate Bank Secrecy Act and anti-money laundering (BSA/AML) and compliance training that is timely and appropriate to their duties.
- Liquidity policies and procedures do not include a method to identify payment-related liquidity needs and the means to meet those needs.
- Planned growth in payment products, services, or delivery channels is not well-developed, is not reasonable, or does not align with the bank's risk appetite.
- The risk assessment process does not capture all the payment products and services that the bank offers and the channels and technologies used.

References

Examples of references that may assist directors in their oversight of payment systems:

Regulations	• 12 CFR 204, "Reserve Requirements of Depository Institutions (Regulation D)" • 12 CFR 210, "Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfer Through Fedwire (Regulation J)" • 12 CFR 229, "Availability of Funds and Collection of Checks (Regulation CC)" • 12 CFR 235, "Debit Card Interchange Fees and Routing (Regulation II)" • 12 CFR 1005, "Electronic Funds Transfer (Regulation E)"

Comptroller's Handbook	• "Compliance Management Systems" • "Corporate and Risk Governance" • "Credit Card Lending" • "Electronic Fund Transfer Act" • "Merchant Processing" • "Payment Systems and Funds Transfer Activities" (national banks)
OTS Examination Handbook	• Section 580 – Payments Systems Risk (FSAs)
OCC bulletins	• 2006-39, "Automated Clearing House Activities: Risk Management Guidance" • 2008-12, "Payment Processors: Risk Management Guidance" • 2009-4, "Remote Deposit Capture: Interagency Guidance" • 2011-26 "Authentication in an Internet Banking Environment: Supplement" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 2016-18, "Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement" • 2017-7, "Third-Party Relationships: Supplemental Examination Procedures" • 2017-43 "New, Modified, or Expanded Bank Products and Services: Risk Management Principles" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
Other	• *FFIEC Information Technology Examination Handbook* – "E-Banking" – "Information Security" – "Outsourcing Technology Services" – "Retail Payment Systems" – "Supervision of Technology Service Providers" – "Wholesale Payment Systems" • "Federal Reserve Policy on Payment System Risk," as amended effective September 15, 2017

Audit Programs

An effective, independent internal and external audit program provides assurance to the board and senior management on the quality of the bank's internal controls and on the effectiveness of risk management, financial reporting, management information systems, and governance practices. The bank's asset size determines if an audit committee is required and also has implications on the composition of the committee.[41] Ultimately, the board is responsible for staying apprised of material audit findings and recommendations, and for holding management accountable for taking sustainable corrective actions to address issues identified by auditors and regulators.

Sources of Information

Examples of sources of information that directors review to oversee the audit program:

- Audit policies
- Audit risk assessments
- Audit universe
- Audit schedules
- Activity reports for audits completed, in process, deferred, and canceled
- Engagement letters
- Third-party relationship reviews for audit firms
- Organizational chart
- Audit issue status reports
- Significant accounting practices and issues
- Internal and external quality assurance reviews
- Audit budget
- Audit staffing and training reports
- Whistleblower complaint reports
- Regulatory reports and communications
- Audit reports

Measures

Examples of measures that directors review to oversee the audit program:

- Percentage of audit reviews completed, in process, deferred, past due, and canceled
- Percentage of corrective actions past due
- Percentage of repeat audit findings
- Percentage of audit validations completed for corrective actions of material deficiencies
- Percentage of corrective actions with multiple target date postponements
- Internal audit staffing and training measures

[41] For more information, refer to 12 CFR 363, "Annual Independent Audits and Reporting Requirements."

Questions to Consider

Examples of questions that directors may consider in their oversight of the audit program:

- Is the audit staff, both internal and external, properly trained and experienced?
- What challenges exist in current or planned audit activities? Is audit coverage sufficient to meet the risks and demands posed by current and planned activities?
- What is the process for completing the audit risk assessment? Who is involved? Does it include all lines of business?
- How does the audit committee meet financial expertise or specialized qualifications to effectively perform its duties?
- What is the root cause for past-due, deferred, or canceled audits, repeat findings, or corrective actions?
- If the external auditor's report expresses a qualified opinion, adverse opinion, or disclaimer of opinion, why?
- Who is responsible for monitoring, tracking, and confirming that corrective actions are implemented? What is the process for validating the effectiveness of corrective actions?

Red Flags

Examples of red flags for directors regarding the audit program:

- The internal audit function lacks stature, authority, independence, competence, resources, or qualifications to perform its duties.
- Internal audit does not adhere to the audit plan or frequently changes the plan without adequate support.
- There is a large number of deferred, past-due, or canceled audits.
- The audit program is not risk-based or does not provide appropriate coverage.
- The audit risk assessment does not include all auditable areas (e.g., excludes low-risk areas) or is not updated to reflect changes or modifications in regulations, products, or services.
- For in-house audit functions, the chief audit executive or chief auditor, if applicable, does not report directly to the board or its audit committee.
- For outsourced audit functions (internal and external), the board and management, in their respective roles, do not exercise the appropriate due diligence before entering into third-party relationships and fail to engage in effective oversight and controls afterward.
- Audit firms change unexpectedly or frequently.
- The external and internal audit firm is one and the same.

- Internal or external auditors do not assess the adequacy of the bank's internal controls system.
- The external or outsourced internal audit firm has conflicts of interest or performs non-audit services for the bank.
- The audit committee lacks the expertise or specialized qualifications to effectively perform its duties.
- There are indications that management controls or inhibits communications from audit staff to the board.
- The audit committee does not comply with applicable composition and independence requirements.
- The audit committee or an independent party does not periodically review the audit work papers to verify the scope was completed as engaged, audit procedures are appropriate, audit conclusions and findings are supported, and staff is qualified.
- Work papers do not provide an adequate audit trail or support audit conclusions.
- Management responses to audit findings are indifferent, noncommittal, or untimely, or do not result in sustainable corrective actions.
- Audit reports identify repeat concerns.
- Root causes are not identified or appropriately analyzed to assist in reducing or eliminating reoccurrences.
- Regulators consistently find issues that are not identified by internal or external auditors.

References

Examples of references that may assist directors in their oversight of the audit program:

Laws	• Pub. L. 107-204, 116 Stat. 745 (2002), Sarbanes–Oxley Act of 2002
Regulations	• 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness" • 12 CFR 162, "Accounting and Disclosure Standards" (FSAs) • 12 CFR 363, "Annual Independent Audits and Reporting Requirements"
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Corporate and Risk Governance" • "Internal and External Audits" • "Internal Control" (national banks) • "Large Bank Supervision"
OTS Examination Handbook	• Section 340, "Internal Control" (FSAs)

Laws	• Pub. L. 107-204, 116 Stat. 745 (2002), Sarbanes–Oxley Act of 2002
OCC bulletins	• 1992-42, "Interagency Policy Statement—External Auditors" • 1999-37, "Interagency Policy Statement on External Auditing Programs" • 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing" • 2016-2, "Interagency Advisory on External Audits of Internationally Active U.S. Financial Institutions"
Other	• *FFIEC Information Technology Examination Handbook* – "Audit" • Basel Committee on Banking Supervision – "Framework for Internal Control Systems in Banking Organisations," September 1998 – "The Internal Audit Function in Banks," June 2012 – "External Audits of Banks," March 2014 – "Corporate Governance Principles for Banks," July 2015 • Committee of Sponsoring Organizations of the Treadway Commission – "Internal Control—Integrated Framework," May 2013 • Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing

As of March 2025, references to reputation risk have been removed from this publication. Refer to OCC Bulletin 2025-4.

Compliance Management System

Banks must comply with applicable laws and regulations. A bank's compliance management system (CMS) should extend beyond consumer protection-related laws and regulations and encompass all applicable laws and regulations, as well as prudent ethical standards and contractual obligations. All banks, regardless of size, should have a CMS that is commensurate with the risk inherent in the bank's products and services. The board should understand the legal and regulatory framework applicable to the bank's activities as well as the potential consequences of violations of laws and regulations that could result in enforcement actions (including civil money penalties), customer reimbursements, financial losses, and increased strategic risk.

Sources of Information

Examples of sources of information that directors review to oversee the CMS:

- Compliance policies
- Compliance risk profile
- Compliance risk assessments
- Compliance audit plans
- Regulatory change management reports
- New activities reports
- Issues status reports
- Regulatory reports and communications
- IRM reports, including compliance monitoring or testing results
- Quality control reports
- Quality assurance reports
- Violations of law and regulations
- Inventory of critical third-party relationships
- Complaint reports
- Whistleblower complaint reports
- Audit reports
- Training reports
- Organizational chart
- Staffing reports

Measures

Examples of measures that directors review to oversee the CMS:

- Violation measures
- Complaint measures
- Issues status measures
- Training completion measures
- New activities measures

As of March 2025, references to reputation risk have been removed from this publication. Refer to OCC Bulletin 2025-4.

Questions to Consider

Examples of questions that directors may consider in their oversight of the CMS:

- How has the bank created a culture that places a priority on compliance? Do the board and management clearly communicate that compliance with all laws and regulations is an organizational priority for all employees?
- What is management's process for identifying the scope and implications of laws, rules, and regulations? What is management's process for identifying prescribed practices; internal policies and procedures; ethical standards; and contractual obligations that apply to the bank and its activities, including those performed by third parties?Is legal counsel involved as appropriate?
- What are the potential consequences of violations, enforcement actions, civil money penalties, customer reimbursements and financial losses?
- What is the chief compliance officer's role, accountability, authority, stature, and qualifications? To whom does the chief compliance officer report?
- What type of recurring compliance-related training do employees and the board receive? Is the training program tailored to job duties and department? How frequent is training? Does training include how to record and escalate complaints?
- What is the bank's change management process for new or amended regulatory requirements?
- What compliance-related activities are outsourced to third parties, and how does management determine whether the bank is complying with the applicable laws and regulations?
- For products or services offered through third parties, how does bank management determine compliance with applicable laws and regulations?
- What is the bank's complaint resolution process? How does the process incorporate complaints enterprise-wide? How does management monitor complaints from outside sources, such as regulators?
- What is the process for employees to report significant concerns to senior management or the board?

Red Flags

Examples of red flags for directors regarding the CMS:

- The board does not receive periodic reports on the bank's state of compliance.
- The CMS does not include a process for identifying, aggregating, and reporting enterprise-wide compliance risks.
- Employee turnover is significant, compliance functions are understaffed, or there is a general lack of stature or expertise in compliance personnel or the chief compliance officer.
- Employees do not receive compliance-related training on a recurring basis, or the training is not tailored to job duties.
- A regulatory change management process is not in place to address new or amended laws and regulations.
- There are deficiencies in risk-based compliance testing activities, monitoring systems, or quality control and quality assurance reviews.
- Compliance issues are not fully considered when new activities are planned or introduced.
- There is no well-defined escalation, tracking, or resolution process in place for compliance issues.
- Significant weaknesses identified in compliance reviews or audits have not been corrected in a timely manner, or there are repeat findings.
- There is no mechanism in place for employees to escalate material compliance issues to the board.
- Compliance risk assessments are not updated to reflect changes to laws, regulations, products, services, or third-party relationships.
- Planned mergers or acquisitions do not consider compliance implications, including an assessment of whether the bank is inheriting any compliance weaknesses(e.g., as evidenced by violations, audit findings, or enforcement actions against the target bank).
- For larger or more complex banks, the board does not receive comprehensive enterprise-wide compliance reporting.
- The complaint resolution process is not well-defined; is not commensurate with the bank's size, complexity, and risk profile; or may result in complaints going unreported or unresolved.
- Violations, compliance review, or audit findings are significant or on an increasing trend.

References

Examples of references that may assist directors in their oversight of the CMS:

Laws	• 12 USC 5531, "Prohibiting Unfair, Deceptive, or Abusive Acts or Practices"[42] • 12 USC 5536, "Prohibited Acts"[43] • 15 USC 45, "Unfair Methods of Competition Unlawful; Prevention by Commission"[44]
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Corporate and Risk Governance" • "Insider Activities" • "Internal and External Audits" • "Internal Control" (national banks) • "Large Bank Supervision" • *Consumer Compliance* series • *Securities Compliance* series
OTS Examination Handbook	• Section 340, "Internal Control" (FSAs) • Section 1300, "Consumer Affairs Laws and Regulations" (FSAs) • Section 1400, "Compliance Laws and Regulations" (FSAs) • Section 1500, "Community Reinvestment Act" (FSAs)
OCC Advisory Letters	• 2002-3, "Guidance on Unfair or Deceptive Acts or Practices"
OCC bulletins	• 2007-31, "Prohibition on Political Contributions by National Banks: Updated Guidance" • 2013-29, "Third-Party Relationships: Risk Management Guidance" • 2014-42 "Credit Practices Rules: Interagency Guidance Regarding Unfair or Deceptive Credit Practices" • 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles" • 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
Other	• Basel Committee on Banking Supervision – "Compliance and the Compliance Function in Banks," April 2005

[42] Section 1031 of the Dodd-Frank Act, which prohibits unfair, deceptive, or abusive acts or practices (UDAAP) is codified at 12 USC 5531.

[43] Section 5536 of the Dodd-Frank Act, which prohibits UDAAP, is codified at 12 USC 5536.

[44] Section 5 of the Fair Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices (UDAP), is codified at 15 USC 45.

Bank Secrecy Act/Anti-Money Laundering

The BSA is intended to safeguard the U.S. financial system and the banks that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. The BSA requires banks to establish a written BSA/AML program to meet its record-keeping and reporting requirements and to confirm the identity of bank customers.[45] The board must approve the bank's BSA compliance program.[46]

Sources of Information

Examples of sources of information that directors review to oversee BSA/AML:

- BSA/AML compliance program (often in the form of a BSA/AML policy), including customer identification program[47]
- BSA/AML risk assessment
- Risk appetite
- Office of Foreign Assets Control (OFAC) policies
- OFAC risk assessment
- Reports regarding SARs
- Reports regarding currency transaction reports (CTR) and CTR exemptions
- Wire transfer reports
- ACH reports
- Reports regarding higher-risk products, services, customers, and geographies
- Fraud loss reports
- Monetary instrument reports
- Cash intensive business reports
- Training reports
- Suspicious activity monitoring system validation reports
- BSA independent testing (e.g., audit reports)

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

[46] For more information, refer to 12 CFR 21.21(c), "Establishment of a BSA Compliance Program."

[47] For more information, refer to 31 CFR 1020.220, "Customer Identification Programs for Banks, Savings Association, Credit Unions, and Certain Non-Federally Regulated Banks," and 12 CFR 21.21(c)(2), "Customer Identification Program."

Measures

Examples of measures that directors review to oversee BSA/AML:

- SAR measures
- Suspicious activity monitoring alert statistics
- Fraud measures
- CTR measures
- Training completion measures
- Measures regarding higher-risk products, services, customers, and geographies
- OFAC monitoring alert statistics
- Law enforcement requests and subpoena statistics

Questions to Consider

- Examples of questions that directors may consider in their oversight of BSA/AML:
- Does the bank have a comprehensive BSA/AML program?
- What controls and monitoring systems are in place for timely detection and reporting of suspicious activities?
- How does management periodically verify that the bank's suspicious activity monitoring system is working as intended?
- If suspicious activity monitoring systems have any gaps, what alternative monitoring methods exist to address those gaps?
- What processes are in place for the filing of SARs, CTRs, and CTR exemptions?
- How is the bank meeting BSA regulatory record-keeping and reporting requirements? How effective is the supporting technology infrastructure?
- How does management verify that timely updates are made to systems, process, policies, and employee training material when there are changes in the BSA's implementing regulations?
- How is customer due diligence conducted?
- What type of BSA/AML and OFAC training are employees and the board receiving to remain aware of their responsibilities under the BSA regulations and internal policy guidelines? Is the training job-specific and relevant to the different functional areas within the bank?
- What type of independent testing is completed to determine compliance with the BSA?

Red Flags

Examples of red flags for directors regarding BSA/AML:

- Findings from IRM, auditors, or regulators indicate the bank's system of internal controls, independent testing, a specific person to coordinate and monitor the BSA/AML compliance program, or training of appropriate personnel for BSA/AML compliance is inadequate.

- The BSA/AML program is not written, board-approved, updated when appropriate, or in line with the BSA/AML risk assessment.
- The BSA/AML and OFAC risk assessments are not updated appropriately or do not accurately reflect all products, services, customers, entities, transactions, and geographic locations unique to the bank.
- The BSA officer changes frequently or lacks the stature, authority, or expertise to manage BSA compliance.
- The BSA staff's skill levels or training are not commensurate with the level of complexity or sophistication of the bank's operations and BSA compliance risk profile.
- Systems used to monitor accounts for suspicious activity are insufficient to keep pace with the transaction volumes.
- Automated systems are used to monitor suspicious activity, but the systems are not customized to reflect the bank's BSA/AML risk profile.
- There are frequent or unsupported changes to the suspicious activity monitoring alert thresholds.
- Alerts generated by the automated system are not reviewed in a timely manner, there is a backlog of alerts to be reviewed, or alerts are cleared without the appropriate analysis or investigation.
- Large-value ACH transactions are initiated through third parties by originators that are not bank customers.
- Higher-risk customers are not properly identified or monitored.
- The volume of SARs or CTRs is very high or low.
- Significant increases in law enforcement requests and subpoenas.
- Ongoing customer due diligence is not in line with the customer's risk profile.
- Bank personnel are not properly trained or do not receive ongoing training on the BSA/AML compliance program and how to identify possible suspicious activity.
- The board does not receive periodic BSA/AML training.
- The board is not notified about filed SARs.[48]
- The board does not receive sufficient information about BSA/AML program weaknesses.
- The bank's customer identification program does not allow the bank to form a reasonable belief that it knows the true identity of each customer.

[48] For more information, refer to 12 CFR 21.11(h), "Notification to Board of Directors" (national banks), and 12 CFR 163.180(d)(9), "Notification to Board of Directors" (FSAs).

References

Examples of references that may assist directors in their oversight of BSA/AML:

Laws	• Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 USC 5311 et seq.) (Bank Secrecy Act)
Regulations	• 12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act (BSA) Compliance" • 12 CFR 21.11, "Suspicious Activity Report" (national banks) • 12 CFR 163.180, "Suspicious Activity Reports and Other Reports and Statements" (FSAs). • 31 CFR Chapter V, "Office of Foreign Assets Control, Department of the Treasury" • 31 CFR Chapter X, "Financial Crimes Enforcement Network, Department of the Treasury" • 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" • 31 CFR 1020.220, "Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks"
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Corporate and Risk Governance" • "Internal and External Audits" • "Large Bank Supervision"
OCC bulletins	• 2005-15, "Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Providing Banking Services to Money Services Businesses" • 2005-16, "Bank Secrecy Act/Anti-Money Laundering: Frequently Asked Questions (updated): Final Customer Identification Program Rule" • 2005-19, "Bank Secrecy Act/Anti-Money Laundering: Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States"

Laws	• Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 USC 5311 et seq.) (Bank Secrecy Act)
OCC bulletins	• 2006-4, "Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Sharing Suspicious Activity Reports with Controlling Companies" • 2007-34, "Bank Secrecy Act/Anti-Money Laundering: Suspicious Activity Report (SAR) Supporting Documentation" • 2007-36, "Bank Secrecy Act/Anti-Money Laundering: BSA Enforcement Policy" • 2007-37, "Bank Secrecy Act/Anti-Money Laundering: Requests by Law Enforcement for Financial Institutions to Maintain Accounts" • 2010-11, "Bank Secrecy Act/Anti-Money Laundering: Beneficial Ownership Guidance" • 2011-9, "Bank Secrecy Act/Anti-Money Laundering: Guidance on Accepting Accounts From Foreign Embassies, Consulates and Missions" • 2012-30, "BSA/AML Compliance Examinations: Consideration of Findings in Uniform Rating and Risk Assessment Systems" • 2016-6, "Bank Secrecy Act/Anti-Money Laundering: Process for Administrative Enforcement Actions Based on Noncompliance With BSA Compliance Program Requirements or Repeat or Uncorrected BSA Compliance Problems" • 2016-32, "Risk Management Guidance on Periodic Risk Reevaluation of Foreign Correspondent Banking" • 2018-35, "Bank Secrecy Act/Anti-Money Laundering: Order Granting Exemption From Customer Identification Program Requirements for Premium Finance Lending" • 2018-36, "Bank Secrecy Act/Anti-Money Laundering: Interagency Statement on Sharing Bank Secrecy Act Resources" • 2018-44, "Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing" • 2019-33, "Bank Secrecy Act/Anti-Money Laundering: Joint Statement on the Risk-Focused Approach to BSA/AML Supervision" • 2019-61, "Bank Secrecy Act/Anti-Money Laundering: Joint Statement on Providing Financial Services to Customers Engaged in Hemp-Related Businesses"
Other	• *FFIEC BSA/AML Examination Manual*

Asset Quality and Credit Risk

Asset quality is a function of the quantity of existing and potential credit risk associated with the loan and investment portfolios, other real estate owned, other assets, and off-balance-sheet transactions. Whether due to lax credit standards, excessive concentrations, weak loan portfolio management, or weakness in the economy, asset quality problems have historically been the major cause of bank losses and failures.

Sources of Information

Examples of sources of information that directors review to oversee asset quality and credit risk management:

- Lending policies
- Credit risk profile
- Underwriting guidelines
- Compensation policies
- Income statement
- Balance sheet
- Loan risk rating reports
- Credit scoring reports
- Investment risk rating reports
- ALLL or ACL methodology and balance
- Rating migration reports
- Credit score migration reports
- Concentration reports
- Supervisory loan-to-value reports[49]
- Insider loan reports
- Delinquent, nonaccrual, nonperforming, and charged-off loan reports
- Renegotiated and restructured loan reports
- Policy exception reports
- Loan participation reports
- Large borrower reports
- Approved appraiser list
- Loan segmentation reports
- Out-of-territory lending reports Risk-layering reports
- Stress-testing reports
- Other real estate owned reports
- Complaint reports
- Whistleblower complaint reports
- Overdraft reports
- Repossessed asset reports
- IRM reports, including credit risk review reports
- Audit reports

[49] Refer to 12 CFR 34, appendix A to subpart D, "Interagency Guidelines for Real Estate Lending."

Measures

Examples of measures that directors review to oversee asset quality and credit risk management:

- Classified and special mention assets to tier 1 capital plus the ALLL or ACL
- Loan growth and changes in portfolio mix
- Portfolio credit quality measures
- Borrower credit quality measures
- Credit concentrations
- Yield on loans and securities
- Foreclosure and repossessed asset measures
- ALLL or ACL to total loans and leases
- Past-due, nonaccrual, nonperforming, and charged-off loans and leases to total loans and leases
- Net losses to average loans and leases
- ALLL or ACL coverage of net losses
- Extension measures
- Modification measures
- Policy exception measures

Questions to Consider

Examples of questions that directors may consider in their oversight of asset quality and credit risk management:

- How does management confirm that proposed changes to lending policies and underwriting standards conform to the stated risk appetite?
- What processes are in place to confirm compliance with credit-related strategies, policies, risk limits, ratios, and applicable laws and regulations, including those pertaining to legal lending limits, appraisals, and insiders?
- How is loan officer compensation determined? Does compensation appropriately balance risk and reward to prevent incentives to expose the bank to imprudent risk and to prevent incentives to engage in unethical business development?
- What are the bank's processes for periodically reviewing loans to confirm the accuracy of risk ratings or credit scoring? At what frequency are loans reviewed? Is the established dollar threshold for reviews appropriate?
- What type of credit analysis and documentation is conducted on loan purchases, including participations?
- What is the root cause of increases in past-due, charge-off, special mention, or classified assets? Is the increase limited to a specific industry, line of business, or loan type, or does the increase apply to the portfolio as a whole?

Red Flags

Examples of red flags for directors regarding asset quality and credit risk management:

- The bank's lending policies do not reflect the board's risk appetite, provide the framework for achieving asset quality and earnings objectives, set risk tolerance levels, or guide the bank's lending activities in a manner consistent with the bank's strategic direction.
- Lending policies do not include appropriate underwriting and risk selection standards consistent with the board's risk appetite.
- There are violations of regulations for lending limits or insider transactions.
- The credit department, including the chief credit officer, and loan administration (back office) do not have the level of staff, expertise, or reports to effectively oversee the loan portfolio.
- Excessive out-of-territory lending, lending outside of the bank's expertise, or granting loans are not in line with lending policies and the board's risk appetite.
- Growth rates in total loans or within individual loan categories are high.
- Loan approval authorization levels are not commensurate with the experience of the lender, type, amount of credit, or level of risk involved.
- Loan officer compensation is tied heavily to growth or volume targets and does not consider quality factors or loan performance.
- Customer or whistleblower complaints indicate potential inappropriate sales practices related to loans that could affect consumers' understanding of or ability to meet repayment obligations.
- Senior management does not identify or report concentrations of credit, or inadequate portfolio segmentation prevents accurate identification of concentrations.
- Concentrations are not evaluated as a percentage of capital to assess magnitude of risk.
- Concentrations exceed established limits with no plans in place to reduce exposure to acceptable levels.
- The bank does not conduct its own due diligence before purchasing loans, including loan participations, syndications, pools, or portfolios.
- There is an overreliance on collateral or borrower characteristics rather than cash flow and income capacity to repay as support for credit decisions.
- Loans granted or renewed with exceptions to policy, procedures, or underwriting guidelines are high or increasing.

- Internal loan risk ratings or credit scoring, including identification of problem loans, are untimely or inappropriate.
- Management does not actively manage problem credits or develop sufficient workout strategies.
- There are downward trends in risk ratings among pass credits and increasing levels of special mention or classified assets.
- The levels of past-due, nonaccrual, nonperforming, extended, deferred, renewed, or rewritten loans are increasing.
- While the ALLL or ACL balance is stable or declining, the overall growth, problem or lower-scoring loans, or other risk indicators are trending upward.
- There is a lack of documentation and analysis to support the ALLL or ACL methodology.
- Credit risk review results show significant risk rating changes.
- The appraisal review function is not independent of the loan production process.
- The loan approval process does not establish accountability for credit quality or approval limits are not appropriate.
- Lending policies, risk management systems, or internal controls have not been revised to keep pace with loan growth or new lending activities.

References

Examples of references that may assist directors in their oversight of asset quality and credit risk management:

Regulations	• 12 CFR 31, "Extensions of Credit to Insiders and Transactions with Affiliates" • 12 CFR 32, "Lending Limits" • 12 CFR 34, "Real Estate Lending and Appraisals" (national banks: subparts A, B, and D; national banks and FSAs: subparts C and E) • 12 CFR 160, "Lending and Investment" (FSAs) • 12 CFR 223, "Transactions Between Member Banks and Their Affiliates (Regulation W)" • 12 CFR 1026, "Truth in Lending (Regulation Z)"
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Corporate and Risk Governance" • "Insider Activities" • "Truth in Lending Act" • "Large Bank Supervision" • "Asset Quality" category of the *Safety and Soundness* series
OTS Examination Handbook	• Section 201, "Overview: Lending Operations and Portfolio Risk Management" (FSAs)

Regulations	• 12 CFR 31, "Extensions of Credit to Insiders and Transactions with Affiliates" • 12 CFR 32, "Lending Limits" • 12 CFR 34, "Real Estate Lending and Appraisals" (national banks: subparts A, B, and D; national banks and FSAs: subparts C and E) • 12 CFR 160, "Lending and Investment" (FSAs) • 12 CFR 223, "Transactions Between Member Banks and Their Affiliates (Regulation W)" • 12 CFR 1026, "Truth in Lending (Regulation Z)"
OCC Banking Circulars	• BC-181, "Purchases of Loans in Whole or in Part-Participations"
OCC bulletins	• 2000-20, "Uniform Retail Classification and Account Management Policy: Policy Implementation" • 2001-37, "Policy Statement on Allowance for Loan and Lease Losses Methodologies and Documentation for Banks and Savings Institutions" • 2006-46, "Concentrations in Commercial Real Estate Lending, Sound Risk Management Practices: Interagency Guidance on CRE Concentration Risk Management" • 2006-47, "Allowance for Loan and Lease Losses (ALLL): Guidance and Frequently Asked Questions (FAQs) on the ALLL" • 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies" • 2010-42, "Sound Practices for Appraisals and Evaluations: Interagency Appraisal and Evaluation Guidelines" • 2011-30, "Counterparty Credit Risk Management: Interagency Supervisory Guidance" • 2012-10, "Troubled Debt Restructurings: Supervisory Guidance on Accounting and Reporting Requirements" • 2013-9, "Guidance on Leveraged Lending" • 2014-29, "Risk Management of Home Equity Lines of Credit Approaching the End-of-Draw Periods: Interagency Guidance" • 2014-55, "Frequently Asked Questions for Implementing March 2013 Interagency Guidance on Leveraged Lending" • 2018-39, "Appraisals and Evaluations of Real Estate: Frequently Asked Questions" • 2019-17, "Current Expected Credit Losses: Additional and Updated Interagency Frequently Asked Questions on the New Accounting Standard on Financial Instruments–Credit Losses" • 2019-43, "Appraisals: Appraisal Management Company Registration Requirements" • 2020-49, "Final Interagency Policy Statement on Allowance for Credit Losses" • 2020-50, "Credit Risk: Interagency Guidance on Credit Risk Review Systems" • 2020-54, "Small-Dollar Lending: Interagency Lending Principles for Offering Responsible Small-Dollar Loans"

Mortgage Banking

Mortgage banking generally involves loan originations as well as purchases and sales of loans through the secondary mortgage market. Banks participate in the secondary market to gain flexibility in managing their long-term interest rate risk exposure, increase liquidity, control credit risk, and expand opportunities to earn fee income. Banks can sell loans directly to government-sponsored entities and private investors, convert loans into mortgage-backed securities, or sell the loan servicing rights. Banks can also sell loans and retain the servicing rights.

Sources of Information

Examples of sources of information that directors review to oversee mortgage banking:

- Mortgage banking policies
- Compensation policies
- Income statement
- Balance sheet
- Profitability reports
- Operational efficiency reports
- Mortgage pipeline reports
- Monthly production volume reports
- Loan inventory aging reports
- Mark-to-market analyses
- Vintage analyses
- Status of reserves
- Repurchase reports
- Quality control reports
- Quality assurance reports
- Policy exception reports
- Investor reviews
- Accounting reports
- Valuation of mortgage servicing assets
- Litigation reports
- Complaint reports
- Staffing reports
- IRM reports
- Audit reports

Measures

Examples of measures that directors review to oversee mortgage banking:

- Profitability measures
- Prepayment ratios
- Warehouse turn rates (e.g., average days in warehouse)
- Hedge coverage[50]
- Earnings-at-risk
- Value-at-risk
- Pull-through and fall-out rates
- Put-back rates
- Foreclosure ratios
- Delinquency ratios
- Loss ratios
- Repurchase measures
- Complaint measures
- Violation measures
- Policy exception measures

[50] Hedge coverage refers to the portion of the rate-sensitive mortgage pipeline and warehouse that a hedging instrument covers.

Questions to Consider

Examples of questions that directors may consider in their oversight of mortgage banking:

- What processes are in place to verify compliance with mortgage banking-related strategies, policies, risk limits, ratios, or applicable laws and regulations?
- What is the credit culture and lending philosophy of the mortgage banking unit? To what degree is it willing to relax credit standards or offer below-market pricing to increase mortgage production volume?
- How are staffing levels and expertise assessed in consideration with origination volumes, servicing size, and the complexity of operations?
- How is compensation determined for mortgage banking managers and staff? Does it appropriately balance risk and reward to prevent incentives to expose the bank to imprudent risk and to prevent incentives to engage in unethical business development?
- What process is in place for developing, approving, and periodically reassessing valuation model assumptions?
- How does the bank ensure compliance with applicable laws and regulations?
- What is the bank's complaint resolution process?

Red Flags

Examples of red flags for directors regarding mortgage banking activities:

- Mortgage banking policies do not define permissible mortgage banking activities, include risk limits, require segregation of duties, address appraisal and investor requirements, outline quality control activities, or define controls for fraud identification and mitigation.
- The quality control function is not independent of the production function or reports to an individual involved in the origination of loans.
- The appraisal review function is not independent of the loan production process.
- Mortgage banking managers' and staff compensation are tied to short-run growth or volume targets and do not consider short and long-term risk.
- Production volume has rapidly changed without corresponding changes in staff and systems.
- The volume of stale loans in the mortgage inventory or retained loans that were intended to be sold are high or increasing.
- Gains or losses on the sale of mortgage loans are disproportionate to the sales volume.
- There is no repurchase reserve or the repurchase reserve analysis is insufficient to support the repurchase reserve.

- Prepayment speeds, discount rates, and other assumptions in mortgage servicing asset valuation models are not supported.
- Retention benefits, deferred tax benefits, captive reinsurance premiums, and income from cross-selling activities are included in valuation models without adequate support from market data.
- Valuation models have not been validated.
- Management has not addressed weaknesses identified by model validation activities in a timely or appropriate manner.
- Mortgage servicing assets are not properly stratified for impairment testing purposes.
- The number of violations or complaints has significantly increased relative to the amount of production and servicing without an adequate assessment of root causes or processes to address them.
- The level of mortgage servicing assets relative to capital is high.
- There are unauthorized exceptions to bank policies, or the level of authorized exceptions is high or increasing.
- There is not adequate documentation in place for all aspects of mortgage banking, including systems to track and collect required mortgage loan documents.
- The compliance review scope does not include a review of compliance with applicable laws and regulations regarding loan originations.

References

Examples of references that may assist directors in their oversight of mortgage banking activities:

Laws	• 12 USC 371, "Real Estate Loans" (national banks) • 12 USC 1464(c), "Loans and Investments" (FSAs)
Regulations	• 12 CFR 7, "Activities and Operations" (national banks: all provisions except 12 CFR 7.1023 and 7.4010; FSAs: 12 CFR 7.1000, 7.1023, 7.3001, and 7.4010) • 12 CFR 30, "Safety and Soundness Standards" • 12 CFR 30, appendix C, "OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices" • 12 CFR 34, "Real Estate Lending and Appraisals" (national banks: subparts A, B, and D; national banks and FSAs: subparts C and E) • 12 CFR 160, "Lending and Investment" (FSAs) • 12 CFR 1008, "S.A.F.E. for Mortgage Licensing Act—State Compliance and Bureau Registration System (Regulation H)" • 12 CFR 1024, "Real Estate Settlement Procedures Act (Regulation X)" • 12 CFR 1026, "Truth in Lending (Regulation Z)"

Laws	• 12 USC 371, "Real Estate Loans" (national banks) • 12 USC 1464(c), "Loans and Investments" (FSAs)
Comptroller's Handbook	• "Corporate and Risk Governance" • "Mortgage Banking" • "Residential Real Estate Lending" • "SAFE Act" • "Truth in Lending Act" • "Unfair or Deceptive Acts or Practices and Unfair, Deceptive, or Abusive Acts or Practices"
OTS Examination Handbook	• Section 201, "Overview: Lending Operations and Portfolio Risk Management" (FSAs)
OCC Advisory Letters	• 2002-3, "Guidance on Unfair or Deceptive Acts or Practices" • 2003-2, "Guidelines for National Banks to Guard Against Predatory and Abusive Lending Practices"
OCC bulletins	• 2003-9, "Interagency Advisory on Mortgage Banking" • 2006-41, "Guidance on Nontraditional Mortgage Product Risks" • 2007-26, "Statement on Subprime Mortgage Lending" • 2010-24, "Interagency Guidance on Sound Incentive Compensation Policies" • 2010-30, "Reverse Mortgages: Interagency Guidance" • 2010-42, "Sounds Practices for Appraisals and Evaluations: Interagency Appraisal and Evaluation Guidelines" • 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" • 2013-38, Interagency Statements on Supervisory Principles for Qualified and Non-Qualified Mortgage Loans" • 2018-39, "Appraisals and Evaluations of Real Estate: Frequently Asked Questions" • 2019-28, "Mortgage Lending: Risk Management Guidance for Higher-Loan-to-Value Lending Activities in Communities Targeted for Revitalization" • 2019-36, "Mortgage Lending: Lending Standards for Asset Dissipation Underwriting"

Liquidity

Liquidity is a bank's capacity to readily meet its cash and collateral obligations at a reasonable cost. Maintaining an adequate level of liquidity depends on the bank's ability to efficiently meet expected and unexpected funding needs without adversely affecting the bank's daily operations or financial condition. Liquidity exists in assets readily convertible to cash, net operating cash flows, and a bank's ability to acquire funding through deposits, borrowings, and capital injections. Funds management involves estimating and planning for liquidity demands over various periods and considering how funding requirements may evolve under various scenarios, including adverse conditions. Banks should maintain sufficient levels of cash, liquid assets, and prospective borrowing lines to meet expected and contingent liquidity demands.

Sources of Information

Examples of sources of information that directors review to oversee liquidity:

- Liquidity policies
- Liquidity risk profile
- Liquidity plans
- Income statement
- Balance sheet
- Asset/liability management reports
- Pro-forma cash flow reports, such as projected sources and uses reports
- Scenario analysis
- Reports on collateral positions
- Contingency funding plan (CFP)
- Results of the CFP tests
- Reports of off-balance sheet exposures
- Stress testing reports and results
- Policy exception reports
- Concentration reports
- Cost of funds reports
- IRM reports
- Audit reports

Measures

Examples of measures that directors review to oversee liquidity:

- Net non-core funding dependence
- Net loans and leases to deposits
- Net loans and leases to assets
- Short-term assets to short-term liabilities
- Diversification targets
- Pledged securities to total securities
- Core deposits to total assets
- Liquid asset coverage ratio
- Liquidity coverage ratio[51]
- Measures on level of borrowings
- Measures on brokered deposits
- Measures on exposures to single fund providers
- Measures on unfunded loan commitments

Questions to Consider

Examples of questions that directors may consider in their oversight of liquidity:

- What processes are in place to confirm compliance with liquidity-related strategies, policies, policies, and risk limits?
- What complement of measurement tools, including forward-looking risk measures and stress scenarios, are provided to the board?
- Do cash flow projections include cash flows from assets, liabilities, and off-balance-sheet items over an appropriate set of time horizons? Are assumptions reasonable?
- How does management support the amount of liquidity needed to support operations, inclusive of unforeseen events?
- At what frequency is the CFP tested?

Red Flags

Examples of red flags for directors regarding liquidity:

- There is an absence of cash flow projections for sources and uses of funds over several time frames and under alternative scenarios.
- Cash flow projection assumptions are unreasonable or unsupported.
- There is no CFP.
- The CFP does not make quantitative assessments of funding needs under events, identify funding sources in response, or outline reporting and communication processes.

[51] The full liquidity coverage ratio requirement generally applies to advanced approaches banking organizations and to their depository institution subsidiaries with total consolidated assets equal to $10 billion or more, Refer to OCC Bulletin 2019-52, "Applicability Thresholds for Regulatory Capital and Liquidity Requirements: Final Rule."

- The bank is engaged in significant payment, settlement, or clearing activities but only manages intraday liquidity under normal conditions and does not consider stressed scenarios.
- The CFP does not include plausible stress events, which affects the accuracy and reasonableness of quantitative projections and expected cash flows.
- The CFP or contingent funding sources are not tested with appropriate frequency.
- Capital ratios are below well-capitalized levels as defined in 12 CFR 6, "Prompt Corrective Action."[52]
- The bank lacks defined authorities and responsibilities for managing the bank's liquidity risk.
- There are declining levels of liquidity, including cash, liquid assets, or availability on borrowing lines.
- There is a significant increase or decrease in funding sources or availability.
- There is significant or increasing reliance on wholesale funding.
- Funding costs have significantly increased.
- Rapid asset growth is funded with rate- or credit-sensitive funding sources.
- There are excessive funding concentrations from a single source or multiple sources with a common rate or credit sensitivity.
- There is an imbalance of funding, such as funding short-term assets with long-term liabilities or long-term assets with short-term liabilities containing embedded options.
- There are large purchases in brokered funds or other potentially volatile sources.
- The liquidity risk profiles of significant subsidiaries and affiliates are largely unknown, inadequately understood, or not considered by management.
- The bank's liquidity risks and current liquidity position are not understood or are not periodically reviewed by management.
- The size of the liquid asset cushion does not align with the risk tolerance and risk profile. There are no limitations to funding sources, like brokered deposits, given the bank's financial condition.

[52] For more information on potential liquidity constraints that can occur when a bank is less than well-capitalized restrictions, refer to OCC Bulletin 2018-33, "Prompt Corrective Action: Guidelines and Rescissions."

References

Examples of references that may assist directors in their oversight of liquidity:

Regulations	• 12 CFR 50, "Liquidity Risk Measurement Standards" (not applicable to community banks) • 12 CFR 204, "Reserve Requirements of Depository Institutions (Regulation D)" • 12 CFR 206, "Limitations on Interbank Liabilities (Regulation F)" • 12 CFR 337.6, "Brokered Deposits"
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Corporate and Risk Governance" • "Large Bank Supervision" • "Liquidity"
OCC bulletins	• 2003-36, "Liquidity Risk Management: Interagency Advisory on the Use of the Federal Reserve's Primary Credit Program in Effective Liquidity Management" • 2004-2, "Banks/Thrifts Providing Financial Support to Funds Advised by the Banking Organization or Its Affiliates: Interagency Guidance" • 2007-21, "Supervision of National Trust Banks: Revised Guidance: Capital and Liquidity" (trust banks) • 2010-13, "Final Policy Statement: Interagency Policy Statement on Funding and Liquidity Risk Management" • 2010-16, "Final Guidance: Interagency Guidance on Correspondent Concentration Risks" • 2017-44, "Liquidity Coverage Ratio: Interagency Frequently Asked Questions"
Other	• Basel Committee on Banking Supervision – "Principles for Sound Liquidity Risk Management and Supervision," September 2008 – "The Liquidity Coverage Ratio and Restricted-Use Committed Liquidity Facilities," January 2014

Interest Rate Risk

IRR is the risk to current or projected financial condition and resilience arising from movements in interest rates. IRR results from timing differences in the repricing of earning assets and interest-bearing liabilities (repricing risk), changing rate relationships among different yield curves of pricing indexes (basis risk), variations in the movement of interest rates along the yield curve (yield curve risk), and interest-related options embedded in bank products (options risk). Each financial transaction that a bank completes may affect its IRR profile; therefore, sound IRR management practices should be in place.

Sources of Information

Examples of sources of information that directors review to oversee IRR:

- Asset/liability management reports, such as
  - gap reports
  - earnings at risk reports
  - economic value of equity reports
- IRR policies
- IRR profile
- Income statement
- Balance sheet
- Stress testing reports and results
- Scenario analysis
- Sensitivity analysis
- Model back-testing results
- Policy exception reports
- Model validation reports
- Model assumptions
- Audit reports

Measures

Examples of measures that directors review to oversee IRR:

- Long-term assets to total assets
- Non-maturity deposits to long-term assets
- Residential real estate loans to total assets
- Investment portfolio depreciation
- Investment portfolio duration
- Net income at risk
- Net interest income at risk
- Economic value of equity
- Periodic and cumulative gap positions

Questions to Consider

Examples of questions that directors may consider in their oversight of IRR:

- What are the level and trends of the bank's IRR exposure?
- How does management identify, measure, monitor, and control IRR, including those IRR from new activities?
- How does the bank measure the potential effect of changes in market interest rates on earnings and capital?

- What processes are in place to confirm compliance with IRR-related strategies, plans, policies, and risk limits?
- What process is in place for developing, approving, and periodically reassessing model assumptions?
- How did management determine the reasonableness and sensitivity of assumptions, including the beta and decay rates for non-maturity deposits and loan prepayment assumptions?
- How does management determine the effectiveness and accuracy of the IRR model? Is the model independently validated and back tested?

Red Flags

Examples of red flags for directors regarding IRR:

- There are significant changes in net interest income.
- Management is using the same assumptions in up and down rate scenarios or across all interest rates.
- Management is not testing more severe IRR scenarios despite historically low- or high-rate environments.
- There are frequent or unsupported changes to the model assumptions.
- Contractual caps and floors and off-balance-sheet items are inaccurately captured in the IRR model.
- There is a high or increasing volume of assets and liabilities with embedded options or fixed-rate loans.
- The duration of the investment portfolio has extended.
- The bank uses derivative-based hedging but does not have management with sufficient expertise regarding these instruments and their potential risks.
- The bank does not have an independent review or validation of its IRR.
- IRR models have not been independently validated.
- Model validation does not include an assessment of the reasonableness of scenarios and assumptions.
- Management has not addressed weaknesses identified by model validation activities in a timely or appropriate manner.
- Model back-testing is not conducted.
- The effects of new strategies are not estimated or stress tested before implementation.
- For banks with elevated exposure to rate-sensitive non-interest income source, management does not measure net income at risk.
- IRR exposures are not stress tested using appropriate scenarios, including meaningful interest rate shocks.
- Management does not use reporting limits, triggers, or thresholds for stress scenarios, including severe rate shocks, to confirm IRR exposures are within risk tolerance levels.

References

Examples of references that may assist directors in their oversight of IRR:

Regulation	• 12 CFR 163.176, "Interest Rate Risk Management Procedures" (FSAs)
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Corporate and Risk Governance" • "Interest Rate Risk" • "Investment Securities" (national banks) • "Large Bank Supervision" • "Risk Management of Financial Derivatives"
OTS Examination Handbook	• Section 540, "Investment Securities" (FSAs) • Section 660, "Derivative Instruments and Hedging" (FSAs)
OCC Banking Circulars	• BC-277, "Risk Management of Financial Derivatives"
OCC bulletins	• 1999-2, "Risk Management of Financial Derivatives and Bank Trading Activities—Supplemental Guidance" • 2004-29, "Embedded Options and Long-Term Interest Rate Risk" • 2009-15, "Investment Securities: Risk Management and Lessons Learned" • 2010-1, "Interagency Advisory on Interest Rate Risk Management" • 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" • 2012-5, "FAQs on 2010 Advisory on Interest Rate Risk Management" • 2015-35, "Risk Management of Financial Derivatives: Quantitative Limits on Physical Commodity Transactions"
Other	• Basel Committee on Banking Supervision – "Interest Rate Risk in the Banking Book," April 2016

Investment Portfolio

Banks may own investment securities and money market funds to help manage asset and liability positions, maintain a liquidity cushion, meet pledging requirements, and diversify their earning streams and balance-sheet composition. Oversight of investment portfolio activities is an important part of managing the bank's interest rate, liquidity, and credit risk profiles.

Sources of Information

Examples of sources of information that directors review to oversee the investment portfolio:

- Investment policies
- Income statement
- Balance sheet
- Asset/liability management reports
- Security purchases and sales reports
- Classified investment reports
- Other-than-temporary impairment analyses
- Pledged securities reports
- Portfolio analytics reports
- Portfolio sensitivity analysis
- List of securities brokers and dealers
- Schedule of par, book, and market value
- Policy exception reports
- IRM reports
- Audit reports

Measures

Examples of measures that directors review to oversee investment portfolio management:

- Concentration analysis
- Maturity measures
- Classified investments as a percentage of capital
- Other-than-temporary impairment
- Investment portfolio duration
- Investment portfolio yields
- Portfolio appreciation/depreciation
- Percentage of investments pledged

Questions to Consider

Examples of questions that directors may consider in their oversight of investment portfolio management:

- How does management determine that individuals with designated investment authority have the expertise to manage the risks associating with investing?
- How is the investment portfolio summarized and how are its risk and return illustrated?

- How is management determining the interest rate sensitivity of investments?
- What is management's strategy behind designating securities as held-to-maturity or available-for-sale?
- What information is management using to determine if an investment should be classified and if there is other-than-temporary impairment?
- What ongoing monitoring activities of the investment portfolio and securities are in place?

Red Flags

Examples of red flags for directors regarding investment portfolio management:

- Investment policies do not describe the board's investment goals; address authorized investment activities and instruments; discuss internal controls and independent review; outline selecting brokers or dealers; include risk limits; or address risk and performance measurement, reporting, and accounting and taxation.
- Investment policies do not include adequate risk diversification or limits on concentrations.
- Investment authorities are not clearly defined or are granted to individuals without the expertise to competently invest or to third parties without management conducting its own independent analysis.
- Securities are purchased without appropriate pre-purchase analysis, or the pre-purchase analysis does not consider all applicable risk exposures.
- There is no estimation of portfolio valuation sensitivities.
- Management relies solely on ratings from nationally recognized statistical rating organizations to determine if the security is investment grade.
- There is a high volume of investments below investment grade.[53]
- The investment portfolio has a significant level of depreciation.
- There are purchases of securities with yields well above market levels or peer group averages.

[53] For more information, refer to OCC Bulletin 2013-28, "Classification of Securities: Interagency Guidance."

- There are purchases of complex structured securities without the technical expertise to understand the structure, embedded options, and interest rate sensitivity.
- There is a sale of securities previously designated as held-to-maturity or transfer of securities from held-to-maturity to available-for-sale.

References

Examples of references that may assist directors in their oversight of investment portfolio management:

Laws	• 12 USC 24, "Corporate Powers of Associations" (national banks) • 12 USC 1464(c), "Loans and Investments" (FSAs)
Regulations	• 12 CFR 1, "Investment Securities" (national banks) • 12 CFR 44, "Proprietary Trading and Certain Interests in and Relationships With Covered Funds" • 12 CFR 160, "Lending and Investment" (FSAs)
Comptroller's Handbook	• "Corporate and Risk Governance" • "Investment Securities" (national banks) • "Risk Management of Financial Derivatives"
OTS Examination Handbook	• Section 540, "Investment Securities" (FSAs) • Section 660, "Derivative Instruments and Hedging" (FSAs)
OCC bulletins	• 1998-20, "Investment Securities: Policy Statement" • 2002-19, "Unsafe and Unsound Investment Portfolio Practices: Supplemental Guidance" (national banks) • 2002-39, "Investment Portfolio Credit Risks: Safekeeping Arrangements: Supplemental Guidance" (national banks) • 2009-11, "Other-Than-Temporary Impairment Accounting: OCC Advisory on Financial Accounting Standards Board Changes" • 2009-15, "Investment Securities: Risk Management and Lessons Learned" (national banks) • 2012-18, "Alternatives to the Use of External Credit Ratings in the Regulations of the OCC: Final Rules and Guidance" • 2013-28, "Classification of Securities: Interagency Guidance" • 2014-27, "Volcker Rule: Interim Examination Procedures"

As of March 2025, references to reputation risk have been removed from this publication. Refer to OCC Bulletin 2025-4.

Asset Management

Asset management is the business of providing financial products or services to a third party for a fee or commission. Activities include traditional fiduciary, retail brokerage, investment company, and custody and security-holder services. These services may be provided in-house, through subsidiaries and affiliates, or through an unaffiliated third party. Asset management activities can expose the bank to financial loss, lost business, litigation, and compliance issues when it fails to fulfill its fiduciary or contractual responsibilities. A bank with fiduciary powers must have a suitable audit of significant fiduciary activities under the direction of a fiduciary audit committee.[54]

Sources of Information

Examples of sources of information that directors review to oversee asset management activities:

- Asset management policies
- Compensation policies
- Income statement
- Balance sheet
- New business reports
- Lost business reports
- Investment performance reports
- Financial performance analyses
- Profitability reports
- Non-credit losses
- Policy exception reports
- Account or asset review reports
- Conflicts of interest reports
- Litigation reports
- Complaint reports
- Compliance reports
- Audit reports
- Fiduciary audit committee charter

Measures

Examples of measures that directors review to oversee asset management activities:

- Accounts opened and closed
- Account and business line profitability measures
- Accounts with non-approved investments
- Account review measures
- Complaint measures
- Conflicts of interest measures
- Compliance testing measures
- Violation measures
- Number of accounts by account type
- Market value of accounts by account type

[54] For information about audit requirements, refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook*. For more information about fiduciary activity-related audit requirements, refer to 12 CFR 9.9, "Audit of Fiduciary Activities" (national banks), and 12 CFR 150.440–150.480, "Audit Requirements" (FSAs).

Questions to Consider

Examples of questions that directors may consider in their oversight of asset management activities:

- Is the asset management line of business meeting the established financial goals and objectives? Why or why not?
- How does management verify that a culture of ethics and accountability is in place?
- How do compensation structures deter imprudent risk or unethical business development?
- How do internal controls protect against fraud, loss, errors, and omissions?
- What processes are in place to confirm conformance with asset management-related strategies, plans, policies, risk limits, or ratios? Is there a formal compliance program? Does management perform self-assessments? Are audits performed in a timely manner?
- What is the bank's complaint resolution process?

Red Flags

Examples of red flags for directors regarding asset management activities:

- IRM or audit results indicate poor account administration, conflicts of interest, or other legal or control breaches.
- Account or asset reviews are past due.
- Management engages in fiduciary activities or relationships it lacks the expertise to manage.
- Compensation structures could incentivize overly high risk or unethical business development.
- Losses from asset management activities are elevated relative to the number of accounts and the transaction volume.
- There are purchases or sales of assets between fiduciary accounts and the bank or bank insiders.
- Account types, account balances, or products and services offered have experienced substantial changes or growth.
- There are unexplained or frequent changes in third parties or auditors.

References

Examples of references that may assist directors in their oversight of asset management activities:

Regulations	• 12 CFR 9, "Fiduciary Activities of National Banks" (national banks) • 12 CFR 12, "Recordkeeping and Confirmation Requirements for Securities Transactions" (national banks) • 12 CFR 150, "Fiduciary Powers of Federal Savings Associations" (FSAs) • 12 CFR 151, "Recordkeeping and Confirmation Requirements for Securities Transactions" (FSAs)
Comptroller's Handbook	• "Bank Supervision Process" • "Community Bank Supervision" • "Compliance Management Systems" • "Corporate and Risk Governance" • "Internal and External Audits" • "Internal Control" (national banks) • "Large Bank Supervision" • "Retail Nondeposit Investment Products" • *Asset Management* series
OTS Examination Handbook	• Section 340, "Internal Control" (FSAs)
OCC bulletins	• 2008-10, "Fiduciary Activities of National Banks: Annual Reviews of Fiduciary Accounts Pursuant to 12 CFR 9.6(c)" • 2010-37, "Fiduciary Activities of National Banks: Self-Deposit of Fiduciary Funds" • 2011-11, "Risk Management Elements: Collective Investment Funds and Outsourced Arrangements" • 2016-17, "Compliance With SEC Money Market Fund Rules by Bank Fiduciaries, Deposit Sweep Arrangements, and Bank Investments"

Appendix: Abbreviations

ACH	automated clearing house
ACL	allowance for credit losses
ALLL	allowance for loan and lease losses
BSA/AML	Bank Secrecy Act and anti-money laundering
CAMELS	capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk
CFP	contingency funding plan
CFR	Code of Federal Regulations
CMS	compliance management system
CTR	currency transaction report
FFIEC	Federal Financial Institutions Examination Council
FSA	federal savings association
IRM	independent risk management
IRR	interest rate risk
NACHA	National Automated Clearing House Association
NIM	net interest margin
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
OTS	Office of Thrift Supervision
RCSA	risk and control self-assessment
ROAA	return on average assets
ROE	return on equity
SAR	suspicious activity report
UBPR	Uniform Bank Performance Report
USC	U.S. Code


OFFICE OF THE
COMPTROLLER OF THE CURRENCY