EXHIBIT 106

Comptroller's Handbook

Safety and Soundness

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

Corporate and Risk Governance

Version 2.0, July 2019

Office of the Comptroller of the Currency

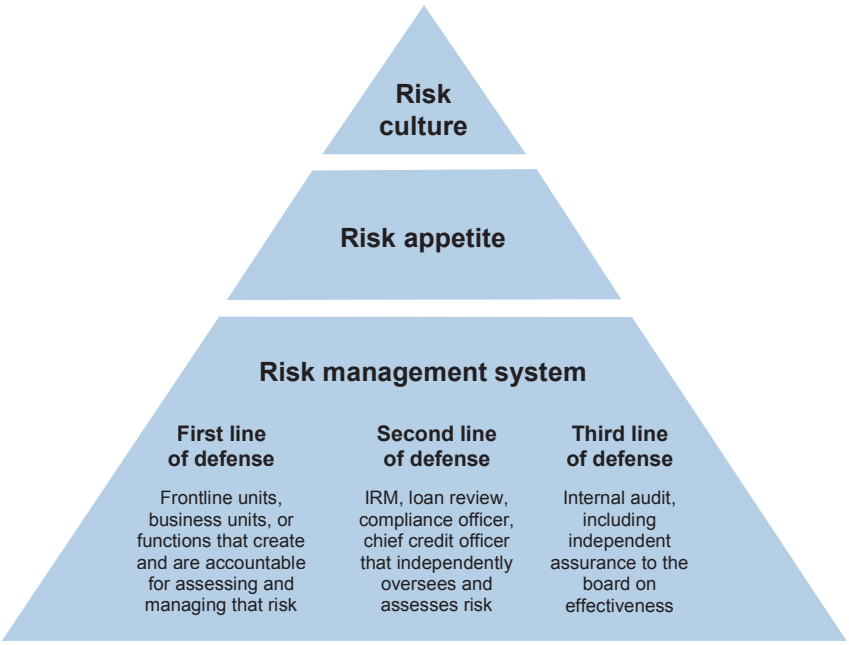
Risk Governance

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

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

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

Figure 1: Risk Governance Framework



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

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

Heightened Standards

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

Risk Culture

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

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

Risk Appetite

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

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

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

[64] Ibid.

[65] Ibid.

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

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

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

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

Heightened Standards

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

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

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

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

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

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

[70] Ibid.

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

Risk Management System

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

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

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

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

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

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

Heightened Standards

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

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

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

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

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

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

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

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

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

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

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

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

Identify Risk

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

Measure Risk

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

Monitor Risk

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

Control Risk

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

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

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

Risk Assessment Process

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

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

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

Policies

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

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

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

Processes

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

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

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

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

Personnel

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

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

[78] Ibid.

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

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

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

Control Systems

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

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

Quality Control

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

Quality Assurance

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

Compliance Management System

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

---

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

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

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

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

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

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

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

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

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

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

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

Bank Secrecy Act/Anti-Money Laundering Program

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

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

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

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

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

---

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

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

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

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

[87] Ibid.

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

Audit Program

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

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

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

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

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

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

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

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

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

Heightened Standards

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

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

Management Information Systems

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

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

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

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

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

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

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

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

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

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

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

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

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

Heightened Standards

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

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

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

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

Third-Party Risk Management

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

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

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

Insurance

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

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

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

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

Insurance Record Keeping

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

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

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

Board and Management's Roles in Risk Governance

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

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

Board's Responsibilities

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

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

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

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

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

Management's Responsibilities

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

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

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

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

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

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

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

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

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

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

Examination Procedures

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

Scope

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

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

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

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

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

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