Risk Management in Enforcement Actions: Managing Risk or Micromanaging It

ABA Banking Law Committee
Enforcement, Insider Liability, and Troubled Banks Subcommittee

Moderators: Dan Stipano, Buckley LLP
Matt Bisanz, Mayer Brown LLP
Agenda

• Panelist Commentary
  • Philip Berkowitz, Shareholder, Littler
  • Irena Gecas-McCarthy, Principal, Deloitte
  • Ed O’Keefe, Member, Moore & Van Allen
  • Liz Ratliff, Assistant Director for Enforcement, Office of the Comptroller of the Currency
  • Megan Webster, Partner, Mayer Brown

• Interactive Discussion
Safety and Soundness

• Banking regulation is intended, in part, to ensure the safety and soundness of banking organizations

• Regulators examine banking organizations to ensure they are operating in a safe and sound manner and complying with applicable laws and regulations
  • Helps to maintain public confidence in the banking system and safeguard the deposit insurance fund

• In the early 1990s, Congress enacted Section 39 of the FDIA, which explicitly requires the federal banking regulators to establish certain safety and soundness standards for insured depository institutions
Section 39 of the FDIA (12 U.S.C. § 1831p–1)

(a) Operational and managerial standards. Each appropriate Federal banking agency shall, for all insured depository institutions, prescribe—

(1) standards relating to—(A) internal controls, information systems, and internal audit systems, in accordance with section 1831m of this title; (B) loan documentation; (C) credit underwriting; (D) interest rate exposure; (E) asset growth; and (F) compensation, fees, and benefits, in accordance with subsection (c); and

(2) such other operational and managerial standards as the agency determines to be appropriate.

(b) Asset quality, earnings, and stock valuation standards. Each appropriate Federal banking agency shall prescribe standards, by regulation or guideline, for all insured depository institutions relating to asset quality, earnings, and stock valuation that the agency determines to be appropriate.

(c) Compensation standards. Each appropriate Federal banking agency shall, for all insured depository institutions, prescribe—

(1) standards prohibiting as an unsafe and unsound practice any employment contract, compensation or benefit agreement, fee arrangement, perquisite, stock option plan, postemployment benefit, or other compensatory arrangement that—(A) would provide any executive officer, employee, director, or principal shareholder of the institution with excessive compensation, fees or benefits; or (B) could lead to material financial loss to the institution;

(2) standards specifying when compensation, fees, or benefits referred to in paragraph (1) are excessive, which shall require the agency to determine whether the amounts are unreasonable or disproportionate to the services actually performed by the individual by considering—(A) the combined value of all cash and noncash benefits provided to the individual; (B) the compensation history of the individual and other individuals with comparable expertise at the institution; (D) comparable compensation practices at comparable institutions, based upon such factors as asset size, geographic location, and the complexity of the loan portfolio or other assets; (E) for postemployment benefits, the projected total cost and benefit to the institution; (F) any connection between the individual and any fraudulent act or omission, breach of trust or fiduciary duty, or insider abuse with regard to the institution; and (G) other factors that the agency determines to be relevant; and

(3) such other standards relating to compensation, fees, and benefits as the agency determines to be appropriate.
Section 39 of the FDIA (cont.)

(d) Standards to be prescribed. (1) In general. Standards under subsections (a), (b), and (c) shall be prescribed by regulation or guideline. Such regulations or guidelines may not prescribe standards that set a specific level or range of compensation for directors, officers, or employees of insured depository institutions.

(e) Failure to meet standards. (1) Plan required. (A) In general. If the appropriate Federal banking agency determines that an insured depository institution fails to meet any standard prescribed under subsection (a) or (b)—
   (i) if such standard is prescribed by regulation of the agency, the agency shall require the institution to submit an acceptable plan to the agency within the time allowed by the agency under subparagraph (C); and
   (ii) if such standard is prescribed by guideline, the agency may require the institution to submit a plan described in clause (i).
Safety and Soundness Standards

• In 1995 and 1996, the federal banking agencies adopted safety and soundness guidelines under Section 39 for all insured depository institution that address:
  • Operational and managerial standards relating to internal controls, information systems, internal audit systems, loan documentation, credit underwriting, interest rate exposure, asset growth, compensation, fees, and benefits
  • Asset quality and earnings standards
  • Compensation standards

• Subsequent interagency safety and soundness guidelines addressed information security and mortgage lending
  • Y2K-related guidelines were adopted in 1998 and repealed in 2001

• Guidelines are enforceable
  • Failure to satisfy the guidelines may result in the institution being required to submit a safety and soundness compliance plan
  • Do not apply to depository institution holding companies
OCC Heightened Standards for Large Institutions

• In 2014, the OCC adopted guidelines to strengthen the governance and risk management practices of large financial institutions
  • Establish minimum standards for the design and implementation of a risk governance framework
  • Also establish minimum standards for board oversight of the framework design and implementation
  • Apply only to national banks, federal thrifts, and insured federal branches of foreign banks with average total consolidated assets of $50 billion or more

• Enforceable under Section 39 of the FDIA

• In 2016, the OCC adopted standalone recovery planning standards for large institutions under its Section 39 authority

• Heightened Standards and recovery planning standards have not been adopted by the Federal Reserve or FDIC for state banks or holding companies
Recent OCC Enforcement Action Items

• Board Supervision and Management; required elements have included:
  • Assessment of board strengths and weaknesses
  • Assessment of current board members and board committee structure
  • Written assessment of management structure and staffing requirements
  • Identification of future senior executive management staffing requirements
  • Clear lines of responsibility and authority for each member of senior executive management
  • Management employment and succession program
  • Process for annually reviewing internal operations, staffing, oversight, information and risk management systems
  • Annual performance appraisal for senior executive officers
Recent OCC Enforcement Action Items (cont.)

• General Risk Management; required elements have included:
  • Written risk governance framework and framework action plan
  • Comprehensive risk control self-assessment requirement for all business units
  • Written compliance risk management program and governance framework

• Credit Risk Management and Independent Loan Review; required elements have included:
  • Formal job descriptions and requirements and performance monitoring
  • Global cash flow and debt service analysis that matches cash flow with debt service for all entities and individuals
  • Risk rating of all loans
  • Independent loan review function that validates credit risk ratings and credit administration processes
Recent OCC Enforcement Action Items (cont.)

• Strategic Plan; required elements have included:
  • Objectives for overall risk profile, earnings, performance, growth, balance sheet mix, off-balance sheet activities, liability structure, capital and liquidity adequacy, financial projections
  • Mission statement, strategic goals and objective, key financial indicators and risk tolerances, SWOT analysis, targeted markets, competitive factors
  • Present and planned products and services and identification and prioritization of initiatives and opportunities
  • Risk management systems, control systems, marketing strategies and partners, funding strategies, management systems and metrics, assigned roles, responsibilities, and accountability
  • Monthly progress review and annual update by board
Recent OCC Enforcement Action Items (cont.)

• Information Technology Governance; required elements have included:
  • Written IT risk assessment and strategy that considers at least eight elements
  • Written IT risk governance plan and risk governance framework
  • IT risk appetite metrics, limits, and risk reporting
  • Comprehensive IT corporate governance guidelines
  • Comprehensive network diagrams and data flows
  • Comprehensive inventory of devices and software licenses
  • Effective enterprise architecture
  • Annual penetration testing on all internet connections
  • Comprehensive IT audit plan
  • Annual board review and revision
Recent OCC Enforcement Action Items (cont.)

• Sales and Marketing Practices Oversight and Governance; required elements have included:
  • Written oversight and governance plan for board and management
  • Controls to ensure clear and consistent definitions of misconduct
  • Clearly defined oversight roles and responsibilities
  • Clearly documented decisions and rationales related to sales and marketing practices

• Products and Services Risk Management; required elements have included:
  • Written analysis following the steps in OCC Bulletin 2004-20
Recent OCC Enforcement Action Items (cont.)

• Mortgage Banking Risk Management; required elements have included:
  • Comprehensive mortgage lending policies and procedures
  • Quality control program that includes monthly testing of samples of loans
  • Comprehensive management information systems to support board and financial statement reporting and compliance and risk management
  • Comprehensive training program

• Leveraged Loan Portfolio; required elements have included:
  • Written program to comply with agency guidance on leveraged lending
  • Leveraged lending underwriting standards at satisfy at least seven elements
  • Periodic stress-testing of enterprise value of individual loans and the portfolio
  • Procedures to aggregate and track leveraged lending exceptions

• Credit Administration; required elements have included:
  • Loan policy that meets 27 requirements
  • “Tickler system” to identify exceptions to the board
Questions for Discussion

• Discuss level of detail in risk management obligations in enforcement actions.

• How granular and/or rigid are the risk management obligations in enforcement actions?

• How do obligations in enforcement actions relate to enterprise-wide risk management efforts, industry best practices, and state law and exchange requirements?

• Should non-covered institutions care about Heightened Standards?
  • Have the Heightened Standards been applied to smaller or non-OCC institutions as a supervisory expectation or best practice?
Audience Questions?
From “Where Were the Lawyers?” to “Where Have the Lawyers Gone?”

July 26, 2019   Ed O’Keefe   Blog, Regulatory Compliance

Colleagues, I hope you are enjoying your summer and have had or are planning a break. Summer breaks help us maintain a healthy balance of rest and work.
Speaking of balance, over a recent beach vacation, I had time to study Tom Baxter’s article on the current role of lawyers in financial institutions: *The Rise of Risk Management in Financial Institutions and a Potential Unintended Consequence – The Diminution of the Legal Function.* Tom analyzes the effect of well-intended post Crisis regulatory governance changes on legal departments. Starting with the three lines of defense, the UK Senior Manager Regime, and heightened standards, Tom examines how the roles of compliance and risk are well defined, while the role of legal is not. Tom also looks to the impact of defining legal risk as a subcategory of operational risk and the prevailing supervisory view that compliance should not report to legal. In Tom’s view, the collective effect of the changes is an increase in the role of risk and compliance and a reduced role for lawyers.

The article has attracted interest from General Counsel as well as their staff and rekindled a long simmering debate in our industry. At a recent breakfast with a senior industry colleague, we discussed Tom’s article and, both of us being of a certain vintage, recalled the 2006 report of a City Bar blue ribbon task force on corporate governance, in which distinguished judges and practitioners considered the then recent spate of corporate scandals (e.g., Enron and World Com). The task force opened its report with Judge Sporkin’s reaction to the Lincoln Savings failure: “Where were the lawyers?” The task force concluded that ‘[t]he role of the General Counsel of a public company is central to an effective system of corporate governance” and recommended changes to enhance the power of in-house lawyers. Fascinating to consider that just over a decade after the City Bar report, we are now debating where the lawyers have gone.

The time has come to consider revising and better defining the role of legal not only within the lines of defense, but also under the bank regulators’ “heightened standards.” Any supervisory view of organizational structures should look to the institution it serves as opposed to a one size fits all approach. While we are at it, let’s also debate why legal risk should not be its own category, rather than swept into a subcategory of operational risk. On the latter point, the timing is auspicious. The Institute of Internal Auditors has issued a draft revision of

www.investigationsandregulatoryadvice.com/from-where-were-the-lawyers-to-where-have-the-lawyers-gone/
the lines of defense and as in the original version, lawyers are not mentioned.

Without improving the current governance construct to explicitly include a legal role, managers may look to their risk functions for legal judgments. Risk should not serve as a filter for the advice of counsel. Risk is not qualified to offer legal judgments on its own and generally its views cannot be privileged. There are also issues uniquely addressed by legal, such as the potential for criminal liability, that go beyond typical risk and compliance considerations. As an industry, if we diminish or exclude legal, we risk losing focus on a key driver of real losses in the post Crisis enforcement period.

While the forgoing is debated, legal functions should consider a few actions and processes to remain fully engaged with management. In my experience, structured, disciplined, and informative reporting processes for legal risk that reaches through the organization can be an effective way to remain engaged. Dashboards, top 10 lists, and regular meeting routines help to keep legal risks in front of management. As the City Bar recommended, “[p]rocesses and procedures should be put in place to ensure that internal lawyers of appropriate seniority are involved in decisions on matters involving disclosure or other legal risk. For example, a company should insure that internal lawyers are present at appropriate meetings or are members of relevant committees.” The legal role is greatly enhanced if management is generally aware of the legal rules for the businesses they manage. Offering the businesses, and most importantly emerging leaders, training on the basic laws and regulations yields significant dividends. Finally, in-house lawyers should also make every effort to engage with risk and compliance functions to understand their reporting and where it is covering legal risk.

At Moore & Van Allen, we continue to engage industry leaders and our clients on the role of legal in corporate governance. We offer boot camps and other learning sessions to teach helpful strategies and tactics.

If you are still looking for a summer read, I am enjoying Phil Knight’s memoir, Shoe Dog. Well done business and personal journey story. Enjoy the rest of your summer.
Regards,

Ed

Ed O'Keefe

Ed O’Keefe, former Global General Counsel of Bank of America Corporation, advises and represents financial institutions. Having also headed or served as a senior executive with Bank of America’s compliance, technology, human resources and operations functions, O’Keefe’s broad experience includes all aspects of investigations litigation, regulatory compliance, governance, cybersecurity, risk management and compensation. O’Keefe’s practice includes advising on all aspects of regulatory compliance, including BSA/AML, anti-bribery/anti-corruption, resolution planning, stress testing and responding to regulatory inquiries. He also advises General Counsel and their leaders on law department management, including engagement with regulators and control functions. A former Deputy General Counsel for Deutsche Bank AG and Chair of The Clearing House Association, O'Keefe has represented financial institutions before the U.S. Congress and the U.K. financial regulatory authorities, global agencies and courts, as well as the Federal Reserve, the Department of Justice, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the Federal Deposit Insurance Corporation and the Equal Employment Opportunity Commission. View Mr. O’Keefe’s full bio.

Share:

Legal Risk, Operational Risk, Regulatory Compliance, Risk Management

SEC Staff Issues Statement on Preparing for Impending LIBOR Transition

Meeks and O'Keefe Article, “Pursuit of a Regulatory Practice Dream: The Story of 2 Powerhouse Bank GCs Uniting,” published by Corporate Counsel
From "Where Were the Lawyers?" to "Where Have the Lawyers Gone?" | MVA White Collar Defense, Investigations, and Regulatory Advisors | 100 North Tryon Street
Suite 4700
Charlotte, NC 28202
1-704-331-1000

DISCLAIMER

Copyright © 2019 Moore & Van Allen PLLC All rights reserved.

Powered by WordPress | Start Magazine by Axle Themes
OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations; Final Rule
DEPARTMENT OF THE TREASURY
Office of the Comptroller of the Currency

12 CFR Parts 30, 168, and 170
[Docket ID OCC–2014–001]

RIN 1557–AD78

OCC Guidelines Establishing
Heightened Standards for Certain
Large Insured National Banks, Insured
Federal Savings Associations, and
Insured Federal Branches; Integration
of Regulations

AGENCY: Office of the Comptroller of the
Currency, Treasury.

ACTION: Final rules and guidelines.

SUMMARY: The Office of the Comptroller
of the Currency (OCC) is adopting
guidelines, issued as an appendix to its
safety and soundness standards
regulations, establishing minimum
standards for the design and
implementation of a risk governance
framework (Framework) for large
insured national banks, insured Federal
savings associations, and insured
Federal branches of foreign banks
(banks) with average total consolidated
assets of $50 billion or more and
minimum standards for a board of
directors in overseeing the Framework’s
design and implementation (final
Guidelines). The standards contained in
the final Guidelines will be enforceable
by the terms of a Federal statute that
authorizes the OCC to prescribe
operational and managerial standards
for national banks and Federal savings
associations. In addition, as part of our
ongoing efforts to integrate the
regulations of the OCC and those of the
Office of Thrift Supervision (OTS), the
OCC is adopting final rules and
guidelines that make its safety and
soundness standards regulations and
guidelines applicable to both national
banks and Federal savings associations
and that remove the comparable Federal
savings association regulations and
guidelines. The OCC is also adopting
other technical changes to the safety and
soundness standards regulations and
guidelines.

DATES: The final rule is effective
November 10, 2014. Compliance dates
for the final Guidelines vary as
specified.

FOR FURTHER INFORMATION CONTACT: Molly Scherf, Deputy Comptroller,
Large Bank Supervision, (202) 649–6210; or Stu Wein, Director, Andra Shuster, Senior Counsel, or
Henry Barkhausen, Attorney, Legislative

\& Regulatory Activities Division, (202)
649–5490, for persons who are deaf or
hard of hearing, TTY, (202) 649–5507;
or Martin Chavez, Attorney, Securities
and Corporate Practices Division, (202)
649–5510, 400 7th Street SW.,
Washington, DC 20219.

SUPPLEMENTARY INFORMATION:

Background

The recent financial crisis demonstrated the destabilizing effect
that large, interconnected financial
companies can have on the national
economy, capital markets, and the
overall financial stability of the banking
system. The financial crisis and the
accompanying legislative response
underscore the importance of strong
bank supervision and regulation of the
financial system. Congress passed the
Dodd-Frank Wall Street Reform and
Consumer Protection Act of 2010 (Dodd-
Frank Act) \(^1\) to address, in part,
weaknesses in the framework for the
supervision and regulation of large U.S.
financial companies.\(^2\) These legislative
developments highlight the view that
large, complex institutions can have a
significant impact on capital markets
and the economy and, therefore, need to
be supervised and regulated more
rigorously.

As a result of the financial crisis, the
OCC developed a set of “heightened
expectations” to enhance our
supervision and strengthen the
governance and risk management
practices of large national banks.\(^3\) These
heightened expectations reflected the
OCC’s supervisory experience during
the financial crisis and addressed
weaknesses the OCC observed in large
institutions’ governance and risk
management practices during this time.

Through its work with the Financial
Stability Board and Basel Committee on
Banking Supervision, the OCC found
that many supervisors are establishing,
or are considering establishing, similar
expectations for the financial
institutions they regulate.\(^4\)


\(^2\) See, e.g., 12 U.S.C. 5365 (requiring enhanced
prudential standards for certain bank holding
companies and nonbank financial companies).

\(^3\) Further background information on the
heightened expectations program is included in the
notice of proposed rulemaking entitled OCC
Guidelines Establishing Heightened Standards for
Certain Large Insured National Banks, Insured
Federal Savings Associations, and Insured Federal
Branches: Integration of Regulations. 79 FR 4282,
4283 (Jan. 27, 2014).

\(^4\) See Financial Stability Board, Thematic Review on
Risk Governance Peer Review Report (Feb. 12,
2013); Principles for An Effective Risk Appetite
Framework (Nov. 18, 2011). See also Basel
Committee on Banking Supervision, Principles for
effective risk data aggregation and risk reporting
(Jan. 2013).

In January 2014, the OCC invited
public comment on proposed rules and
guidelines addressing the following two
topics: (i) Guidelines establishing
minimum standards for the design and
implementation of a Framework for
large insured national banks, insured
Federal savings associations, and
insured Federal branches and minimum
standards for boards of directors
overseeing the Framework of these
institutions (proposed Guidelines); and
(ii) the integration of 12 CFR parts 30
and 170 (proposed integration rules
and integration guidelines).\(^5\)

After carefully considering the
comments we received on the proposed
Guidelines, the OCC is adopting these
final Guidelines as a new Appendix D
to part 30 of our regulations. As
described more fully below, the final
Guidelines supersede the OCC’s
previous heightened expectations program with respect to covered banks.\(^6\)
The OCC, as the primary financial
regulatory agency for national banks and
Federal savings associations, believes
that the final Guidelines further the goal
of the Dodd-Frank Act to strengthen the
financial system by focusing
management and boards of directors on
strengthening risk management
practices and governance, thereby
minimizing the probability and impact
of future crises. In addition, the final
Guidelines will provide greater certainty
to covered banks about the OCC’s risk
management expectations and improve
examiners’ ability to assess compliance
with the standards contained in
Appendix D. The OCC is also adopting
the proposed integration rules and
integration guidelines substantially as
proposed, with minor technical
changes.

We have set forth below a summary
of the comments we received, and a
detailed description of the proposed
Guidelines, significant comments, and
the standards contained in the final
Guidelines.

Notice of Proposed Rulemaking:
Summary of General Comments

The OCC received 25 comment letters
on the proposed Guidelines from
financial institutions and trade
associations, among others, and
received no comment letters on the
proposed integration rules and
integration guidelines. The comments
addressed all major sections of the
proposed Guidelines. To improve
understanding of the issues raised by

\(^5\) 79 FR 4282 (Jan. 27, 2014).

\(^6\) The OCC has adopted a definition of the term
“covered bank” to clarify the scope of the final
Guidelines. This definition is discussed in the
definitions section of this preamble.
commenters, the OCC met with a number of these commenters to discuss issues relating to the proposed Guidelines, and summaries of these meetings are available on a public Web site.7

Many commenters expressed support for the broader goals of the proposed Guidelines. At the same time, other commenters raised concerns with various provisions in the proposed Guidelines. For example, commenters argued that the proposed Guidelines were too prescriptive and requested the OCC to revise the final Guidelines to be more principles-based and to provide additional flexibility in applying the Guidelines to different types of banks.

Some commenters also interpreted the proposed Guidelines as prohibiting banks from utilizing their parent company’s risk governance framework and resources. These commenters noted that this could result in conflicting standards, increased risk, and a duplication of systems and resources and urged the OCC to allow the bank to leverage existing holding company risk management processes.

Commenters also generally opposed categorizing certain organizational units as front line units. These commenters noted that organizational units such as legal, human resources, finance, and information technology do not create duplication of systems and resources and urged the OCC to allow the bank to leverage existing holding company risk management processes.

As discussed more fully below, the OCC has revised the final Guidelines in response to the issues and information provided by commenters, and has made technical changes to the final rule and guidelines integrating 12 CFR parts 30 and 170. These modifications to the final Guidelines and explanations that address comments are described in the section-by-section description of the final Guidelines.

Enforcement of the Guidelines

The OCC is adopting the final Guidelines pursuant to section 39 of the Federal Deposit Insurance Act (FDIA).8 Section 39 authorizes the OCC to issue heightened standards in the form of a regulation or guidelines. For national banks, these standards currently include three sets of guidelines issued as appendices to part 30 of our regulations. Appendix A contains operational and managerial standards that relate to internal controls, information systems, internal audit systems, loan documentation, credit underwriting, interest rate exposure, asset growth, asset quality, earnings, and compensation, fees and benefits. Appendix B contains standards on information security and Appendix C contains standards that address residential mortgage lending practices. The safety and soundness standards for Federal savings associations are found in Appendices A and B to 12 CFR part 170. Part 30, part 170, and Appendices A and B were issued on an interagency basis and are comparable.9

Section 39 prescribes different consequences depending on whether the agency issues regulations or guidelines. Pursuant to section 39, if a national bank or Federal savings association fails to meet a standard prescribed by regulation, the OCC must require it to submit a plan specifying the steps it will take to comply with the standard. If a national bank or Federal savings association fails to meet a standard prescribed by guideline, the OCC has the discretion to require the submission of such a plan.10 The issuance of these heightened standards as guidelines rather than as a regulation provides the OCC with supervisory flexibility to pursue the course of action that is most appropriate given the specific circumstances of a covered bank’s failure to meet one or more standards, and the covered bank’s self-corrective and remedial responses. The OCC has procedural rules contained in part 30 that implement the enforcement remedies prescribed by section 39. Under these provisions, the OCC may initiate the enforcement process when it determines, by examination or otherwise, that a national bank or Federal savings association has failed to meet the standards set forth in the final

Guidelines.12 Upon making that determination, the OCC may request, through letter or Report of Examination, that the national bank or Federal savings association submit a compliance plan to the OCC detailing the steps the institution will take to correct the deficiencies and the time within which it will take those steps. This request is termed a Notice of Deficiency. Upon receiving a Notice of Deficiency from the OCC, the national bank or Federal savings association must submit a compliance plan to the OCC for approval within 30 days.

If a national bank or Federal savings association fails to submit an acceptable compliance plan, or fails materially to comply with a compliance plan approved by the OCC, the OCC may issue a Notice of Intent to Issue an Order pursuant to section 39 (Notice of Intent). The bank or savings association then has 14 days to respond to the Notice of Intent. After considering the bank’s or savings association’s response, the OCC may issue the order, decide not to issue the order, or seek additional information from the bank or savings association before making a final decision. Alternatively, the OCC may issue an order without providing the bank or savings association with a Notice of Intent. In this case, the bank or savings association may appeal after-the-fact to the OCC, and the OCC has 60 days to consider the appeal and render a final decision. Upon the issuance of an order, a bank or savings association will be deemed to be in noncompliance with part 30. Orders are formal, public documents, and they may be enforced in district court or through the assessment of civil money penalties under 12 U.S.C. 1818.

Description of the OCC’s Guidelines Establishing Heightened Standards

The final Guidelines consist of three sections. Section I provides an introduction to the Guidelines, explains the scope of the Guidelines, and defines key terms used throughout the Guidelines. Section II sets forth the minimum standards for the design and implementation of a covered bank’s Framework. Section III provides the minimum standards for the board of directors’ oversight of the Framework.

9 As discussed further below, the OCC is also adopting final rules and guidelines that make part 30 and its appendices applicable to Federal savings associations, and that remove part 170.
10 Section 39 of the FDIA applies to “insured depository institutions,” which would include insured Federal branches of foreign banks. While we do not specifically refer to these entities in this discussion, it should be read to include them.
11 See 12 U.S.C. 1831p–1(e)(1)(A)(i) and (ii). In either case, bankruptcy statute authorizes the issuance of an order and the subsequent enforcement of that order in court, independent of any other enforcement action that may be available in a particular case.
12 For national banks and Federal savings associations, the procedures governing the determination and notification of failure to satisfy a standard prescribed pursuant to section 39, the filing and review of compliance plans, and the issuance, if necessary, of orders are set forth in our regulations at 12 CFR 30.3, 30.4, and 30.5.
Section I: Introduction

Under the proposed Guidelines, the OCC would expect a bank to establish and implement a Framework for managing and controlling the bank’s risk taking. The proposed Guidelines established the minimum standards for the design and implementation of the Framework and the minimum standards for the board of directors in overseeing the Framework’s design and implementation.

The proposed Guidelines permitted a bank to use its parent company’s risk governance framework if the bank has a risk profile that is substantially the same as its parent company’s risk profile, the parent company’s risk governance framework complies with the proposed Guidelines, and the bank demonstrates through a documented assessment that its risk profile and its parent company’s risk profile are substantially the same. The proposed Guidelines provided that the bank should conduct this assessment at least annually or more often in conjunction with the review and update of the Framework performed by independent risk management as set forth in paragraph II.A. of the proposed Guidelines.

Under the proposed Guidelines, a parent company’s and bank’s risk profiles would be considered substantially the same if, as of the most recent quarter-end Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Report), the following conditions are met: (i) The bank’s average total consolidated assets represent 95 percent or more of the parent company’s average total consolidated assets; (ii) the bank’s total assets under management represent 85 percent or more of the parent company’s total assets under management; and (iii) the bank’s total off-balance sheet exposures represent 95 percent or more of the parent company’s total off-balance sheet exposures. As provided in the proposed Guidelines, a bank that did not satisfy this test could submit to the OCC for consideration an analysis that demonstrates that the risk profile of the parent company and the bank are substantially the same based on other factors.

The proposed Guidelines provided that the bank would need to develop its own Framework if the parent company’s and bank’s risk profiles are not substantially the same. The bank’s Framework should ensure that the bank’s risk profile is easily distinguishable from the parent company’s for risk management and supervisory reporting purposes and that the safety and soundness of the bank is not jeopardized by decisions made by the parent company’s board of directors or management.

Several commenters argued that it was inefficient and counterproductive to require a bank to create a second risk framework in addition to the parent company’s framework. According to the commenters, a separate bank-specific risk framework would be isolated from the overall enterprise risk framework and undermine the goals of sound risk management. Other commenters indicated that banks should be allowed to use their parent company’s risk governance framework because the Dodd-Frank Act requires bank holding companies to serve as a source of strength for their insured depository institution subsidiaries.

Some commenters also interpreted the proposed Guidelines to prohibit the bank from using any components of the parent company’s risk governance framework unless the risk profiles of the bank and its parent company are substantially the same. Commenters argued that the OCC should change the threshold for the substantially the same determination from 95 percent to 85 percent. They noted that in certain other regulatory contexts special treatment is granted when the total assets of an insured depository institution comprise 85 percent or more of the assets of its parent company.13 One commenter argued that the current Call Report and holding company reporting forms do not contain parallel line items for assets under management and off-balance sheet exposures, making it problematic to establish that a bank is above the 95 percent threshold under those measures. Several commenters also suggested that the OCC should allow multiple subsidiary banks of a parent company to aggregate their asset sizes in order to meet the 95 percent threshold. The commenters noted that some banking organizations conduct banking activities through multiple charters and that a prohibition on aggregation would result in unnecessary and duplicative risk management programs.

The OCC is making a few modifications to the introductory section. The final Guidelines continue to establish minimum standards for the design and implementation of a covered bank’s Framework and minimum standards for the covered bank’s board of directors in providing oversight of the Framework’s design and implementation. The OCC notes that these standards are not intended to be exclusive, and that they are in addition to any other applicable requirements in law or regulation. For example, the OCC expects covered banks to continue to comply with the operational and management standards articulated in Appendix A to part 30, including those related to internal controls, internal audit systems, risk management, and management information systems.

Paragraph 3. of the final Guidelines clarifies that a covered bank may use its parent company’s risk governance framework in its entirety, without modification, if the framework meets these minimum standards and the risk profiles of the parent company and the covered bank are substantially the same as demonstrated through a documented assessment. The covered bank should conduct this assessment at least annually in conjunction with the review and update of the Framework performed by independent risk management pursuant to paragraph II.A.

Paragraph 4. of the final Guidelines continues to set forth the substantially the same test, but simplifies the test by removing the provisions relating to assets under management and off-balance sheet exposures. Under the final Guidelines, a parent company’s and covered bank’s risk profiles are substantially the same if, as reported on the covered bank’s Call Report for the most recent consecutive quarters, the covered bank’s average total consolidated assets represent 95 percent or more of the parent company’s average total consolidated assets.14 The final Guidelines also provide that a covered bank that does not satisfy this test may submit a written analysis to the OCC for consideration and approval that demonstrates that the risk profile of the parent company and the covered bank are substantially the same based upon other factors.

The OCC has determined not to lower the 95 percent threshold, as suggested by some commenters. The 95 percent threshold in the final Guidelines functions as a safe harbor, above which a covered bank will not need to create its own Framework. If a covered bank and its parent company have substantially the same risk profile, the covered bank can use any and all components of the parent company’s risk governance framework as its own, provided the parent company’s framework complies with the final

14 The final Guidelines clarify that average total consolidated assets for a parent company means the average of the parent company’s total consolidated assets, as reported on the parent company’s Form FR Y–9C to the Board of Governors of the Federal Reserve System (Board), or equivalent regulatory report, for the four most recent consecutive quarters.
Guidelines. A covered bank that does not meet the 95 percent threshold can use components of its parent company’s framework, provided those components meet the criteria outlined in the Guidelines.

The OCC believes a high threshold is necessary to ensure that a covered bank’s Framework appropriately considers the sanctity of each national bank or Federal savings association charter within a parent company’s legal entity structure. During the financial crisis, the OCC and some boards of directors were unable to accurately assess certain national banks’ risk profiles because their respective parent company’s risk management practices were assessing, managing, and reporting risks by line of business, rather than legal entity. In addition, decisions by some parent companies’ boards of directors and management teams leading up to the crisis created unacceptable risk levels in their national bank subsidiaries. As a result, these parent companies were unable to provide financial or other support to their bank subsidiaries despite the fact that a parent company is expected to serve as a source of strength for its bank subsidiaries.

The covered bank’s Framework should ensure that the covered bank’s risk profile is easily distinguished and separate from its parent company for risk management and supervisory reporting purposes and that the safety and soundness of the covered bank is not jeopardized by decisions made by the parent company’s board of directors and management. This includes ensuring that assets and businesses are not transferred into the covered bank from nonbank entities without proper due diligence and ensuring that complex booking structures established by the parent company protect the safety and soundness of the covered bank.

Although the final Guidelines continue to provide that a covered bank should establish its own Framework when the parent company’s and covered bank’s risk profiles are not substantially the same, the Guidelines also clarify that even in these cases a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company’s risk governance framework when developing its own Framework to the extent those components are consistent with the objectives of these Guidelines. It is important to note that neither the proposed Guidelines nor the final Guidelines prohibit a covered bank from using those components of its parent company’s risk governance framework that are appropriate for the covered bank. Indeed, the OCC encourages covered banks to leverage their parent company’s risk governance framework to the extent appropriate, including by using employees of the parent company. For example, it may be appropriate for the same individual to serve as Chief Risk Executive or Chief Audit Executive of a covered bank and its parent company.

We note that the extent to which a covered bank may use its parent company’s framework will vary depending on the circumstances. For example, it may be appropriate for a covered bank to use the parent company’s framework without modification where there is significant similarity between the covered bank’s and parent company’s risk profiles, or where the parent company’s framework provides for focused governance and risk management of the covered bank. Conversely, a covered bank may incorporate fewer components of the parent company’s framework where the risk profiles of the covered bank and parent are less similar, or the parent company’s risk governance framework is less focused on the covered bank. In these situations, it may be necessary to modify components of the parent company’s risk governance framework that the covered bank incorporates or relies on to ensure the bank’s risk profile is easily distinguished from that of its parent and that decisions made by the parent do not jeopardize the safety and soundness of the covered bank. It is expected that the covered bank will consult with OCC examiners to determine which components of a parent company’s risk governance framework may be used to ensure that the covered bank’s Framework complies with the Guidelines.

The OCC recognizes that covered banks operate within their overall parent company’s risk governance framework, and that covered banks may realize efficiencies when their parent company’s risk governance framework is consistent with these Guidelines. However, modifications may be necessary when the parent company’s risk management objectives are different than the covered bank’s risk management objectives. For example, a parent company’s board of directors and management will need to understand and manage aggregate risks that cross legal entities, while a covered bank’s board and management will need to understand and manage only the covered bank’s individual risk profile. The OCC believes these distinct goals and processes are complementary. The covered bank should work closely with its parent company to promote efficiencies and synergies between the two risk governance frameworks.

Scope and Compliance Date

The proposed Guidelines applied to a bank with average total consolidated assets equal to or greater than $50 billion as of the effective date of the Guidelines (calculated by averaging the bank’s total consolidated assets, as reported on the bank’s Call Reports, for the four most recent consecutive quarters). For those banks with average total consolidated assets less than $50 billion as of the effective date of the Guidelines, but that subsequently have average total consolidated assets of $50 billion or greater, the proposed Guidelines applied to such banks on the as-of date of the most recent Call Report used in the calculation of the average.

Several commenters objected to the $50 billion threshold. Some commenters suggested that the OCC increase the threshold to one more consistent with the complexity of the bank and the heightened risk the bank posed. One commenter suggested using the $250 billion threshold in the Basel III advanced approaches. Another commenter favored eliminating the $50 billion threshold and instead adopting a principles-based approach that applies the Guidelines to banks whose operations are highly complex or present a heightened risk.

Some commenters requested that the OCC provide banks not previously subject to the OCC’s heightened expectations program with a year or longer to comply with the final Guidelines. Other commenters argued that the OCC should permit an institution that becomes newly subject to the Guidelines a minimum of two years to achieve full compliance. Several commenters argued that the OCC should allow banks previously subject to the OCC’s heightened expectations program a minimum of one year from the date of the final Guidelines because of the new and more detailed requirements contained in the Guidelines.

The OCC believes that the final Guidelines should apply to any bank with average total consolidated assets equal to or greater than $50 billion.

---

16 The approach for calculating average total consolidated assets under the final Guidelines is the same as that in the proposed Guidelines. Specifically, the final Guidelines provide that average total consolidated assets for a covered bank means the average of the covered bank’s total consolidated assets, as reported on the covered bank’s Call Reports for the four most recent consecutive quarters.
but recognizes that covered banks with assets equal to or greater than $50 billion may differ in the degree of risk they present and, therefore, as described below, we are making several changes to this section to address the compliance date for covered banks based on size and experience with the heightened expectations program. In addition, we note that the $50 billion asset criteria is a well understood threshold that the OCC and other Federal banking regulatory agencies have used to demarcate larger, more complex banking organizations from smaller, less complex banking organizations. Accordingly, the final Guidelines retain the $50 billion threshold.

The OCC is also clarifying that the final Guidelines will apply to any bank with average total consolidated assets less than $50 billion in the limited circumstances where that institution’s parent company controls at least one covered bank. This would include both sister banks of the covered bank as well as covered bank subsidiaries and sister bank subsidiaries that are banks (e.g., insured credit card banks or insured trust banks). The meaning of the terms “bank,” “covered bank,” and “control” is discussed in the Definitions section below.

As noted above, the final Guidelines contain a schedule that phases-in the date for a covered bank to comply with the final Guidelines. A covered bank with average total consolidated assets equal to or greater than $75 billion should comply with the final Guidelines by the effective date, i.e., 60 days after these Guidelines are published in the Federal Register. A covered bank with average total consolidated assets equal to or greater than $100 billion but less than $75 billion as of the effective date should comply with the final Guidelines within six months from the effective date.

A covered bank with average total consolidated assets equal to or greater than $50 billion but less than $100 billion as of the effective date should comply with these Guidelines within 18 months from the effective date. A covered bank with average total consolidated assets less than $50 billion that is a covered bank because that bank’s parent company controls at least one other covered bank as of the effective date should comply with these Guidelines on the same date that such other covered bank should comply. Finally, a covered bank with less than $50 billion in average total consolidated assets on the effective date of the final Guidelines that subsequently becomes subject to the Guidelines because its average total consolidated assets are equal to or greater than $50 billion should comply with the Guidelines within 18 months from the as-of date of the most recent Call Report used in the calculation of the average.

The OCC notes that larger institutions have been subject to the OCC’s heightened expectations program since 2010 and should need less time to comply with the final Guidelines. Other covered banks have been subject to certain aspects of the heightened expectations program and therefore may require additional time to comply with all aspects of the final Guidelines.

Reservation of Authority

In order to maintain supervisory flexibility, the proposed Guidelines reserved the OCC’s authority to apply the Guidelines to a bank whose average total consolidated assets are less than $50 billion if the OCC determines that such bank’s operations are highly complex or otherwise present a heightened risk as to require compliance with the Guidelines. The proposed Guidelines provided that the OCC would consider the complexity of products and services, risk profile, and scope of operations to determine whether a bank’s operations are highly complex or present a heightened risk.

Conversely, the proposed Guidelines also reserved the OCC’s authority to delay the application of the Guidelines to any bank, or modify the Guidelines as applicable to certain banks. Additionally, the proposed Guidelines provided that the OCC may determine that a bank is no longer required to comply with the Guidelines. The OCC would generally make this determination if a bank’s operations are no longer highly complex or no longer present a heightened risk that would require continued compliance with the Guidelines. Finally, the proposal provided that the OCC would apply notice and response procedures, when appropriate, consistent with those set out in 12 CFR 3.404 when exercising any of these reservations of authority.

Some commenters expressed concern about the OCC’s use of reservation of authority to apply the Guidelines to banks below the $50 billion threshold, particularly community banks. Other commenters asserted that the proposed Guidelines should apply to a bank below the $50 billion threshold only when the bank’s risk profile is elevated and the bank has met a list of objective factors.

After reviewing the comments, the OCC is finalizing the reservation of authority paragraph substantially as proposed with minor technical changes. The final Guidelines provide that the OCC reserves the authority to apply the Guidelines, in whole or in part, to a bank below the $50 billion threshold if the OCC determines that the bank’s operations are highly complex or otherwise present a heightened risk. The OCC expects to utilize this authority only if a bank’s operations are highly complex relative to its risk-management capabilities, and notes that “[t]his is a high threshold that only will be crossed in extraordinary circumstances.” The OCC does not intend to exercise this reservation of authority to apply the final Guidelines to community banks.

Consistent with the proposal, the final Guidelines reserve the OCC’s authority to extend the time for compliance with the Guidelines, modify the Guidelines, or to determine that compliance with the Guidelines is no longer appropriate for a particular covered bank. The OCC would generally make this determination if a covered bank’s operations are no longer highly complex or no longer present a heightened risk based on consideration of the factors articulated in the Guidelines. The final Guidelines continue to provide that the OCC will apply notice and response procedures, when appropriate, consistent with those set out in 12 CFR 3.404.

21 See id. ("Some community bankers may be reading that language as a loophole that we will use to impose onerous new requirements on community banks. I want to assure you that this is not the case and not our intent.").
As discussed above, the proposed Guidelines applied to an insured Federal branch of a foreign bank with average total consolidated assets of $50 billion or more. We noted in the preamble to the proposed Guidelines that, pursuant to the reservation of authority, the OCC may modify the Guidelines to tailor them for insured Federal branches due to their unique nature.

Some commenters requested that the OCC delay any decision regarding application of the Guidelines to an insured Federal branch pending a more definite determination of what such tailoring contemplates. In particular, these commenters requested that the OCC clarify the treatment of independent risk management and internal audit, and the role for the foreign banking body under the Guidelines. Some commenters also asserted that the proposed Guidelines did not adequately address that an insured Federal branch does not have a board of directors. Some commenters also argued that the final Guidelines should provide each insured Federal branch considerable flexibility to apply them in a manner best suited to its circumstances.

After reviewing the comments, the OCC has determined that the final Guidelines will apply to insured Federal branches with $50 billion or more in average total consolidated assets. However, the OCC recognizes that insured Federal branches do not have a U.S. board of directors and that their risk governance frameworks will vary due to the variety of activities performed in the branch. As a result, the OCC intends to apply the final Guidelines in a flexible manner to insured Federal branches. For example, if an insured Federal branch were to become subject to these final Guidelines, the OCC would apply the Guidelines in a manner that takes into account the nature, scope, and risk of the branch’s activities. This means that the OCC will consult with the insured Federal branch to adapt the final Guidelines in an appropriate manner to the branch’s operations.

In addition, the final Guidelines omit footnote one from the proposal which provided that, in the case of an insured Federal branch, the board of directors means the managing official in charge of the branch. In the event an insured Federal branch becomes subject to the final Guidelines, OCC examiners will consult with the branch to determine the appropriate person or committee to undertake the responsibilities assigned to the board of directors under the final Guidelines. The OCC continues to expect that all Federal branches have risk governance frameworks in place that are commensurate with the level of risk taken in or outside the U.S. impacting U.S. operations.

**Preservation of Existing Authority**

As discussed above, the final Guidelines are enforceable pursuant to section 39 of the FDIA and part 30 of our rules. Section I of the Guidelines also provides that nothing in section 39 or the Guidelines in any way limits the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law.

**Definitions**

The proposed Guidelines defined several terms, including Chief Audit Executive, Chief Risk Executive, front line unit, independent risk management, internal audit, risk appetite, and risk profile. With the exception of the front line unit definition, the OCC is adopting these definitions substantially as proposed, with certain clarifying and technical changes. The final Guidelines also include definitions for the terms bank, control, and covered bank.

**Bank.** The proposed Guidelines defined the term “bank” in the scope section of the proposed Guidelines to mean any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank with average total consolidated assets equal to or greater than $50 billion as of the effective date of the Guidelines. The OCC is moving this definition to paragraph I.E. Definitions to consolidate all of the definitions in one location. Under the final Guidelines, the term “bank” means any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank. As discussed below, the OCC is also introducing the term “covered bank” to more clearly indicate the types of institutions covered by these Guidelines.

**Chief Audit Executive.** The proposed Guidelines defined the term “Chief Audit Executive” (CAE) as an individual who leads internal audit and is one level below the Chief Executive Officer (CEO) in the bank’s organizational structure. The OCC received no comments and is adopting this definition as proposed with one technical change.

**Chief Risk Executive.** The proposed Guidelines defined the term “Chief Risk Executive” (CRE) as an individual who leads an independent risk management unit and is one level below the CEO in the bank’s organizational structure. The proposal noted that some banks designate one CRE, while others designate risk-specific CRES. In the latter situation, the proposal provided that the bank should have a process for coordinating the activities of all independent risk management units so they can provide an aggregated view of risks to the CEO and the board of directors or the board’s risk committee. The proposal solicited comment on the advantages and disadvantages of having a single CRE versus having multiple, risk-specific CRES.

Some commenters noted that it is advantageous for a single CRE to provide oversight to all independent risk management units, and argued that a single CRE is unnecessary to ensure a cohesive and coordinated approach to risk management. Other commenters asserted that requiring a single CRE would be too prescriptive for the varied risk profiles and organizational designs among banks, and noted that such a requirement may not be appropriate to the size, scale, and complexity of each institution. In addition, these commenters noted that having two or three executives performing CRE functions and having access to the board of directors can provide additional perspective to the board.

After reviewing the comments received, the OCC is adopting the definition substantially as proposed with one clarifying change. The final Guidelines provide that Chief Risk Executive means an individual who leads an independent risk management unit and is one level below the CEO in a covered bank’s organizational structure. The final definition expressly states that a covered bank may have more than one CRE. Because the OCC did not receive compelling information regarding the appointment of a single CRE, we are providing covered banks flexibility in determining the appropriate number of CRES. The OCC continues to believe, however, that a covered bank with multiple, risk-specific CRES should have effective processes for coordinating the activities of all independent risk management units so that they can provide an aggregated view of all risks to the CEO.

---

22 See proposed Guidelines I.A.

23 See 79 FR 4282, 4285 n.15 (Jan. 27, 2014).

24 See final Guidelines paragraph I.E.3.
and the board of directors or the board’s risk committee.

Control. As discussed below, the OCC is adopting a definition of the term “covered bank” to clarify the scope of the final Guidelines. The definition of the term “covered bank” turns, in part, on the definition of “control.” While the concept of control was discussed in the proposed Guidelines, the proposal did not include a definition of this term. The OCC is adopting a definition of the term “control” that is based on the definition provided in 12 CFR 3.2.

Under the final Guidelines, a parent company controls a covered bank if it: (i) Owns, controls, or holds with power to vote 25 percent or more of a class of voting securities of the covered bank; or (ii) consolidates the covered bank for financial reporting purposes. The OCC believes that this definition will assist institutions in determining whether they are a “covered bank,” and therefore subject to the final Guidelines.

Covered Bank. In order to clarify the scope of the final Guidelines, the OCC is adopting a definition of the term covered bank. Under the final Guidelines, the term covered bank means any bank: (i) With average total consolidated assets equal to or greater than $50 billion; (ii) with average total consolidated assets less than $50 billion if that bank’s parent company controls at least one covered bank; or (iii) with average total consolidated assets less than $50 billion, if the OCC determines that the bank’s operations are highly complex or otherwise present a heightened risk as to warrant the application of the final Guidelines. The OCC believes that this definition accurately reflects the scope of the proposed Guidelines, and has made changes throughout the text of the Guidelines to incorporate this term.

Front line unit. The proposed Guidelines defined the term “front line unit” as any organizational unit within the bank that: (i) Engages in activities designed to generate revenue for the parent company or bank; (ii) provides services, such as administration, finance, treasury, legal, or human resources to the bank; or (iii) provides information technology, operations, servicing, processing, or other support to any organizational unit covered by the proposed Guidelines.25

Several commenters strongly opposed this definition claiming that it inappropriately includes organizational units that do not “own” or create risk, such as legal, compliance, finance, human resources, and information technology. These commenters suggested that these types of organizational units mainly perform risk mitigation or support functions and therefore should not be subject to the standards in the Guidelines. Other commenters expressed concern that the proposed definition would subordinate the views of the three organizational units to independent risk management thus, for example, potentially subjecting legal decisions and advice to review by independent risk management and internal audit.

Some commenters also noted that organizational units may have many different functions, only some of which involve accountability for risk that warrants treatment under these Guidelines. One commenter suggested that, in such cases, the OCC classify part of the unit as a front line unit. One commenter suggested that the front line unit definition should include revenue-generating business units and personnel who provide functional support to these units, such as legal advisory services or technology development, when those personnel are compensated by and report into the business unit. Finally, several commenters urged the OCC to provide flexibility to determine how service and support functions should fit into the bank’s risk governance framework.

After carefully considering the comments, the OCC is making several changes to this definition. Under the final Guidelines, a front line unit means, except as otherwise provided, any organizational unit or function thereof in a covered bank that is accountable for one of several enumerated risks and that either: (i) Engages in activities designed to generate revenue or reduce expenses for the parent company or covered bank; (ii) provides operational support or servicing to any organizational unit or function within the covered bank in the delivery of products or services to customers; or (iii) provides technology services to any organizational unit or function covered by these Guidelines. Thus, to meet the definition of a front line unit, an organizational unit or function would need to be accountable for a risk and also meet one of three additional criteria that capture the types of risk-taking activities these Guidelines are intended to address. The final Guidelines also provide that a front line unit does not ordinarily include an organizational unit or function thereof within a covered bank that provides legal services to the covered bank.

The OCC believes that this revised definition provides greater flexibility to identify and classify organizational units or functions thereof that are responsible for risks covered by these Guidelines as front line units. Specifically, this definition makes it possible for part of an organizational unit to qualify as a front line unit without implicating the entire organizational unit. For example, in some institutions, the Chief Financial Officer’s organizational unit may be responsible for setting goals and providing oversight to enterprise-wide expense reduction initiatives. These initiatives have the potential to create one or more risks, if actions taken to achieve cost saving goals inappropriately weaken risk management practices or internal controls. With regard to this responsibility, the finance organizational unit would be a front line unit, subject to the oversight and challenge of independent risk management. However, the finance organizational unit would not be a front line unit with regard to its responsibility to establish, assess, or report on line of business compliance with other enterprise-wide policies and procedures, such as those associated with preparing the covered bank’s financial statements.

The final definition also clarifies that, if an organizational unit or function is accountable for a risk within a covered bank, it is considered a front line unit whether or not it created the risk. The purpose of this change is to make clear that a front line unit’s responsibility for, or ownership of, a risk may arise by engaging in the activity that originally created the risk within the covered bank, or when the organizational unit is assigned accountability for a risk that was created by another organizational unit. For example, accountability for an individual loan or a portfolio of loans and its associated risks may transfer from one organizational unit or function to another within a covered bank. The organizational unit or function that assumes responsibility for the loan or loan portfolio becomes a front line unit.
at the time accountability for the risk is transferred.

Conversely, there may be circumstances where an organizational unit may have some accountability for one or more risks, but may not meet other provisions of the definition and thus would not be a front line unit for purposes of these Guidelines. For example, one of the primary responsibilities of human resources is to design and implement compensation programs, which, if not designed and implemented properly, could motivate inappropriate risk-taking behavior. However, human resources does not meet any of the three additional criteria, and therefore, is not a front line unit for purposes of these Guidelines. The OCC believes excluding human resources from the definition of front line unit is appropriate, given that the compensation programs it designs and implements are designed with input from other organizational units and subject to the review and approval of the board of directors, or a committee thereof. The board of directors may, at its discretion, request input from independent risk management on the design and implementation of the compensation program or individual compensation plans, regardless of whether human resources is a front line unit. Furthermore, the other activities in which human resources engages are not directly related to the types of risks covered by these Guidelines.

The proposed Guidelines provided that an organizational unit that engages in activities designed to generate revenue for the parent company or the bank would be a front line unit. The final Guidelines modify this provision to provide that a front line unit could include an organizational unit or function that engages in activities designed to generate revenue or “reduce expenses.” The purpose of this change is to more effectively include within the front line unit definition certain functions within an organizational unit without including the entire unit. Under the proposal, a front line unit included an organizational unit that “provides information technology, operations, servicing, processing, or other support to any organizational unit covered by these Guidelines.” The OCC notes that, in the revised definition, an organizational unit or function accountable for risk may be a front line unit if it “provides operational or servicing support to any organizational unit or function within the covered bank in the delivery of products or services to customers.” The OCC revised this definition because the proposed definition was too broad and could create issues similar to those raised by commenters with regard to including all aspects of organizational units such as finance, human resources, etc., in the front line unit definition. The revised definition is more focused on the organizational units and functions that the OCC intended to include in the definition of front line unit.

Finally, the OCC agreed with commenters that the definition of a front line unit should not ordinarily include an organizational unit or function thereof that provides legal services to the covered bank. The OCC notes, however, that there may be instances where the General Counsel is responsible for functions that extend beyond legal services. The OCC expects that examiners will determine whether these functions meet the definition of a front line unit, independent risk management, or internal audit and will discuss with covered banks whether any determinations made by the covered bank conflict with the final Guidelines.

Independent risk management. The proposed Guidelines defined the term independent risk management as any organizational unit within the bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. The proposal noted that these units maintain independence from front line units by following the reporting structure specified in the proposed Guidelines. Under the proposal’s reporting structure, the board of directors or the board’s risk committee reviews and approves the Framework and any material policies established under the Framework. In addition, the board of directors or the board’s risk committee approves all decisions regarding the appointment or removal of the CRE and approves the annual compensation and salary adjustment of the CRE. The proposal clarified that the board of directors or the board’s risk committee should receive communications from the CRE on the results of independent risk management’s risk assessments and activities, and other matters that the CRE determines are necessary. The proposal also provided that the board of directors or its risk committee should make appropriate inquiries of management or the CRE to determine whether there are scope or resource limitations that impede the ability of independent risk management to execute its responsibilities.

The proposed definition specified that the CEO oversees the CRE’s day-to-day activities. The proposal clarified that this includes resolving disagreements between front line units and independent risk management that cannot be resolved by the CRE and front line unit(s) executive(s), and overseeing budgeting and management accounting, human resources administration, internal communications and information flows, and the administration of independent risk management’s internal policies and procedures. Finally, the proposed definition provided that no front line unit executive oversees any independent risk management unit.

Some commenters noted that the proposed Guidelines suggest that cooperative or integrated relationships between independent risk management and front line units could undermine the independence of independent risk management. These commenters argued that independent risk management’s effectiveness can be enhanced through active involvement with business units, and that the final Guidelines should recognize the benefits of, and not create impediments to, this engagement.

Commenters also addressed the relationship between a parent company’s and bank’s independent risk management functions. Some commenters noted that the proposal conflicts with other regulatory authorities insofar as those authorities expect risk officers at the bank to report into the parent company’s risk management function, whereas the proposal provided that the CRE of the bank should report to a bank’s CEO. Other commenters expressed the view that the proposed Guidelines appear to require a bank to have a separate chief risk officer and separate risk management organization from its parent company. These commenters argued that requiring risk management activities at the bank separately from the same activities at the parent company would be duplicative and increase compliance costs.

One commenter noted that the provision regarding the CEO’s oversight of the CRE’s day-to-day activities suggested too prescriptive a level of involvement. This commenter noted that while the CEO should be accountable for these activities, he or she should not be required to be personally involved in the day-to-day activities of other executives. This commenter requested the OCC to clarify that the CEO should not be expected to become significantly involved in the details of independent risk management.

29 Id.

30 Id.
The OCC is adopting the definition substantially as proposed with certain modifications to address commenters’ concerns. The final Guidelines provide that independent risk management means any organizational unit within a covered bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks.31

Consistent with the proposal, the final Guidelines articulate a reporting structure that enables independent risk management to maintain its independence from front line units.32 Under this reporting structure, the board of directors or the board’s risk committee reviews and approves the Framework. In addition, the final Guidelines clarify that a CRE should have unrestricted access to the board of directors and its committees with regard to risks and issues identified through independent risk management’s activities. The board of directors or its risk committee approves all decisions regarding the appointment or removal of the CREs and approves the annual compensation and salary adjustment of the CREs. The final definition removes the provision for the CEO to oversee the CRE’s (or CREs’) day-to-day activities. The term day-to-day activities was intended to convey that the CEO would oversee the CRE’s (or CREs’) activities in a manner similar to the oversight the CEO provides to other direct reports. Given the potential for misinterpretation of the term day-to-day, and the fact that this expectation is implied in the CRE’s (or CREs’) reporting structure defined in the Proposed Guidelines, the OCC determined that this additional requirement is not necessary. The final Guidelines continue to provide that no front line unit executive oversees any independent risk management unit. Conversely, the CRE should not oversee any front line unit.

The OCC has also removed from the final definition the provision that the board of directors or the board’s risk committee review and approve any material policies established under the Framework. As discussed below, the OCC did not intend to assign managerial responsibilities to the board of directors or its risk committee. The OCC believes that board or risk committee approval of material policies under the Framework would be burdensome, and that these policies should be approved by management instead. Nevertheless, the OCC continues to believe that the board of directors or the board’s risk committee should receive communications from the CRE on the results of independent risk management’s risk assessments and activities, and other matters that the CRE determines are necessary. In addition, the board of directors or its risk committee should make appropriate inquiries of management or the CRE to determine whether there are scope or resource limitations that impede the ability of independent risk management to execute its responsibilities.

The OCC did not intend the proposed Guidelines to limit interaction between independent risk management and front line units, nor did the OCC intend to imply that the relationship between front line units and independent risk management should be uncooperative or adversarial. Instead, the OCC expects independent risk management to coordinate and to actively engage with front line units. However, the OCC expects that independent risk management will apply its own judgment when assessing risks and the effectiveness of risk management practices within a front line unit. In addition, there may be situations where independent risk management and front line units disagree. As provided in the proposal, the OCC continues to believe that these disagreements should be resolved by the CEO when the CRE and front line unit(s) executive(s) are unable to resolve these issues.

The Guidelines, as proposed and finalized, do not limit or prevent an employee of a covered bank, such as a CRE, from also serving as an officer with the covered bank’s parent company and satisfying reporting requirements applicable to the covered bank’s parent company. Accordingly, if a CRE is also an employee of a covered bank’s parent company, the final Guidelines do not prohibit the CRE from reporting to an executive within the parent company that provided that the executive does not impede the CRE’s independence within the covered bank’s Framework. Similarly, as discussed above, the OCC notes that the final Guidelines clarify that a covered bank may use elements of a parent company’s risk governance framework, but only to the extent that this is appropriate for the covered bank.

**Internal audit.** The proposed Guidelines defined the term internal audit as the organizational unit within the bank that is designated to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B. Similar to the proposed definition of independent risk management, the proposal noted that internal audit maintains independence from front line units and independent risk management units by implementing the reporting structure specified in the proposed Guidelines. Under the proposal’s reporting structure, the board’s audit committee reviews and approves internal audit’s overall charter, risk assessments, and audit plans. In addition, the proposal provided that the audit committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the CAE. The proposal clarified that the audit committee should receive communications from the CAE on the results of internal audit’s activities or other matters that the CAE determines are necessary and make appropriate inquiries of management or the CAE to determine whether there are scope or resource limitations that impede the ability of internal audit to execute its responsibilities.33

The proposed definition also provided that the CEO oversees the CAE’s day-to-day activities. The proposal clarified that the CEO’s oversight responsibilities include, but are not limited to, budgeting and management accounting, human resources administration, internal communications and information flows, and the administration of the unit’s internal policies and procedures.34 The proposed definition also noted that in some banks, the audit committee may assume the CEO’s responsibilities to oversee the CAE’s day-to-day activities, and that this would be acceptable under the proposed Guidelines.35 Finally, the proposed definition provided that no front line unit executive oversees internal audit.

Similar to comments on the proposed definition of independent risk management, comments on the proposed definition of internal audit focused on the organizational unit’s reporting structure. Some commenters argued that the reporting line for the CAE was too narrow and requested that the final Guidelines provide more flexibility to permit the CAE to report to another senior executive (e.g., general counsel) on day-to-day issues. These commenters noted that permitting more flexibility supports the goals of internal audit independence and unfettered access to the bank’s board of directors. Other commenters noted that internal audit and the CAE are most effective and independent when they report functionally to the board of directors or the audit committee and administratively to a suitable executive, such as the CEO.

31 Final Guidelines paragraph I.E.7.
32 Id.
33 79 FR 4287.
34 79 FR 4288.
35 See proposed Guidelines I.C.5 n.2.
Some commenters also expressed the view that the proposed Guidelines would require a banking organization to establish duplicative audit departments for its parent company and each of its banks. These commenters noted that a centralized audit function is more effective and efficient, ensures consistent audit coverage, and enables enterprise-wide functional reviews that help to identify systemic issues quickly. The OCC did not intend to suggest that a covered bank is prohibited from using its parent company’s risk governance framework when their respective risk profiles are not substantially the same. As described more fully above, the final Guidelines generally provide that a covered bank may rely on components of its parent company’s risk governance framework, including internal audit, to the extent those components are consistent with the objectives of the final Guidelines.

One commenter noted that the provision regarding the audit committee’s or CEO’s oversight of the CAE’s day-to-day activities suggested a level of involvement that was too prescriptive and, in the case of the audit committee, too management-oriented. This commenter requested that the OCC modify this provision to recognize that neither the CEO nor audit committee should be expected to become significantly involved in the details of internal audit. Finally, some commenters argued that the audit committee should only review and approve material risk assessments. After reviewing the comments received, the OCC is adopting the definition of internal audit substantially as proposed with certain modifications. As provided in the final Guidelines, the term internal audit means the organizational unit within a covered bank that is designated to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B.

Consistent with the proposal, the final Guidelines articulate a reporting structure that enables internal audit to maintain its independence from front line units and independent risk management. Under the reporting structure included in the final Guidelines, the CAE has unrestricted access to the audit committee with regard to risks and issues identified through internal audit’s activities. In addition, the audit committee reviews and approves internal audit’s overall charter and audit plans. Further, the audit committee approves all decisions regarding the appointment or removal and determination and salary adjustment of the CAE. The final definition clarifies that the audit committee or the CEO oversees the CAE’s administrative activities. Finally, the final definition continues to provide that no front line unit executive oversees internal audit.

The OCC agrees with comments that neither the CEO nor the audit committee need to be involved in the details of the CAE’s daily activities. The final definition preserves this dual reporting structure, and clarifies that the CEO or the audit committee oversees the CAE’s administrative activities, rather than the CAE’s day-to-day activities. This reflects the OCC’s belief that either the CEO or the audit committee should have primary oversight responsibility over the CAE’s administrative activities. These administrative activities include routine personnel matters such as leave and attendance reporting, expense account management, and other departmental matters such as furniture, equipment, and supplies. In addition, revisions made to the definition of front line unit provide internal audit more flexibility to consult with other organizational units, as necessary. For example, the final Guidelines do not prevent internal audit from consulting with a covered bank’s legal unit on legal matters because the legal unit is generally not a front line unit.

The OCC recognizes that the proposed definition could have been interpreted to mean that the audit committee should review and approve all internal audit risk assessments, and agrees with commenters that this could impose operational burdens on the audit committee and detract from their oversight role. Therefore, the final definition removes this provision and clarifies that the audit committee reviews and approves the overall charter and audit plan. When presenting the audit plan to the audit committee for approval, internal audit may include the risk assessments that support the audit plan to assist the committee in carrying out its responsibilities. Finally, the OCC continues to expect that the audit committee should receive communications from the CAE on the results of internal audit’s activities or other matters that the CAE determines are necessary and make appropriate inquiries of management or the CAE to determine whether there are scope or resource limitations that impede the ability of internal audit to execute its responsibilities.

Parent company. The term “parent company” was used throughout the proposed Guidelines. One commenter noted that the term means a variety of different entities within a multi-tiered holding company structure.

The OCC is adopting a definition of the term “parent company” to clarify the final Guidelines. The term parent company means the top-tier legal entity in a covered bank’s ownership structure. Thus, the parent company of a covered bank that is an insured national bank or insured Federal savings association may be a domestic or foreign entity.

Risk appetite. The proposed Guidelines defined the term “risk appetite” as the aggregate level and types of risk the board of directors and management are willing to assume to achieve the bank’s strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements. The OCC received no comments on this definition and is adopting it as proposed with minor technical changes.

Section II: Standards for Risk Governance Framework
Risk Governance Framework

Section II of the proposed Guidelines set minimum standards for the design and implementation of a bank’s Framework. Under paragraphs A. and B., the proposal required a bank to establish and adhere to a formal, written Framework approved by the board of directors or its risk committee that is reviewed and updated at least annually (and as often as needed) by independent risk management to address changes in the bank’s risk profile caused by internal or external factors or the evolution of industry risk management practices. We received no comments on this section, however we are making clarifying changes. We have added a provision stating that the Framework should include delegations of authority from the board of directors to management committees and executive officers as well as risk limits established for material activities. The Framework should also include processes for management’s reports to the board of directors covering policy, limit compliance, and exceptions. In addition, we have added that the review of the Framework should include changes resulting from emerging risks and the covered bank’s strategic plans.
Scope of Risk Governance Framework

Under the proposed Guidelines, the Framework would cover certain specified risk categories that apply to the bank. These categories are credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk.

One commenter requested clarification regarding the meaning of reputation and strategic risk and argued that the OCC should provide additional clarification or remove these two risk types. The final Guidelines continue to include all eight categories of risk, which are described in existing OCC guidance. The OCC recognizes that industry practices for managing reputation and strategic risks are less developed than those associated with other risk categories. However, it is important for boards of directors and management teams to incorporate these risks into their decision-making processes. Therefore, for purposes of the final Guidelines, the OCC expects front line units, independent risk management, and internal audit to consider these risks when carrying out their responsibilities under the Guidelines.

Roles and Responsibilities

Paragraphs II.C.1. through 3. of the final Guidelines set forth the roles and responsibilities for front line units, independent risk management, and internal audit. These units are fundamental to the design and implementation of the Framework. As we noted in the preamble to the proposed Guidelines, they are often referred to as the “three lines of defense” and, together, should establish an appropriate system to control risk taking. These units should keep the board of directors informed of the covered bank’s risk profile and risk management processes to allow the board of directors to provide credible challenges to management’s recommendations and decisions.

37 These roles and responsibilities are in addition to any roles and responsibilities set forth in Appendices A, B, and C to Part 30. Many of the risk management practices established and maintained by a covered bank to meet these standards, including loan review and credit underwriting and administration practices, should be components of its Framework, within the construct of the three distinct units identified in the final Guidelines. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks, e.g., compliance risk management. These risk-specific programs should also be considered components of the Framework, within the context of the three units described in paragraph II.C. of the final Guidelines.

addition, the independent risk management and internal audit units must have unrestricted access to the board, or a committee thereof, with regard to their risk assessments, findings, and recommendations, independent from front line unit management and, when necessary, the CEO. This unrestricted access to the board of directors is critical to the integrity of the Framework.

In carrying out their responsibilities within the Framework, front line units, independent risk management, and internal audit may engage the services of external experts to assist them. This expertise can be useful in supplementing internal expertise and providing perspective on industry practices. However, no organizational unit in the covered bank may delegate its responsibilities under the Framework to an external party.

Many of the commenters expressed support for the lines of defense risk governance structure contained in the proposed Guidelines. Some commenters, however, argued that classifying all of a bank’s activities into one of three lines of defense draws artificial bright lines that ignore the mix of functions performed. Other commenters noted that placing all units other than independent risk management and internal audit in the front line could force banks to significantly modify their organizational structures, reporting lines, and risk control practices and that this could impair banks’ ability to effectively manage risks. A few commenters asked for additional guidance on the reporting structures for compliance and loan review programs.

As discussed earlier, the OCC has revised the definition of front line unit to provide covered banks more flexibility in identifying front line units. The OCC believes that these revisions respond to commenters’ concerns and more closely align the final Guidelines with the traditional “lines of defense” approach. Below, we discuss the role and responsibilities of front line units, independent risk management, and internal audit.

Role and Responsibilities of Front Line Units

Front line units are the first of a bank’s three lines of defense. The proposed Guidelines provided that front line units should take responsibility and be held accountable by the CEO and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. The proposed Guidelines provided that front line units should assess, on an ongoing basis, the material risks associated with their activities. The front line unit should use these risk assessments as the basis for fulfilling the responsibilities that were described in paragraphs (b) and (c) of paragraph II.C.1. of the proposed Guidelines and for determining if they need to take action to strengthen risk management or reduce risk given changes in the unit’s risk profile or other conditions.

Paragraph (b) provided that front line units should establish and adhere to a set of written policies that include front line unit risk limits, as discussed in paragraph II.F. of the proposed Guidelines. The proposed Guidelines provided that these policies should ensure that risks associated with the front line units’ activities are effectively identified, measured, monitored, and controlled consistent with the bank’s risk appetite statement, concentration risk limits, and the bank’s policies established within the Framework pursuant to paragraphs II.C.2.(c) and II.G. through K. of the proposed Guidelines.

Paragraph (c) provided that front line units should also establish and adhere to procedures and processes necessary to ensure compliance with the aforementioned written policies. Paragraph (d) provided that front line units should adhere to all applicable policies, procedures, and processes established by independent risk management.

Finally, the proposed Guidelines provided that front line units should develop, attract, and retain talent and maintain appropriate staffing levels, and establish and adhere to talent management processes and compensation and performance management programs that comply with paragraphs II.L. and II.M., respectively, of the proposed Guidelines.

Some commenters expressed concern that the proposed Guidelines prevent front line units from relying on other organizational units to perform their assigned responsibilities. For example, one commenter argued that the proposed Guidelines could be interpreted as suggesting that front line units have exclusive responsibility for establishing risk limits, a responsibility assigned to independent risk management in many banks. This commenter recommended that the final Guidelines clarify that front line units do not have exclusive responsibility for establishing front line unit risk limits, and that the front line unit may perform this responsibility by or in conjunction with independent risk management. Some commenters suggested that the final Guidelines recognize that a front
line unit may use policies, procedures, and controls established by other organizational units, and that the front line units’ responsibility should be contributing their expertise to the development of those policies, procedures and controls. Some commenters also requested the OCC to clarify how the responsibilities assigned to front line units would apply to legal services or other functions that, in some banks, do not report directly to a business leader.

After reviewing the comments, the OCC is adopting the role and responsibilities of front line units with minor clarifying changes. To allow covered banks some flexibility in designing their Framework, the final Guidelines provide that a front line unit may fulfill its responsibilities either alone or in conjunction with another organizational unit whose purpose is to assist a front line unit in fulfilling its responsibilities under the Framework. In such cases, the Framework should establish appropriate authority and accountability for each responsibility in the Framework, and the organizational unit assisting the front line unit cannot be independent risk management. As the OCC observed during the financial crisis, it can be challenging to instill a sense of “risk ownership” in a front line unit when multiple organizational units are responsible for the risks associated with the front line unit’s activities. Banks whose business leaders viewed themselves as accountable for the risks created through their activities fared better in the crisis than banks where accountability for risks were shared among multiple organizational units. The OCC cautions covered banks that rely on such a structure to be diligent in reinforcing the front line unit’s accountability for the risks it creates.

With respect to paragraph (c) of the final Guidelines, a front line unit’s processes for establishing its policies should provide for independent risk management’s review and approval of these policies to ensure they are consistent with other policies established within the Framework. Within this process, independent risk management would review and approve the front line unit’s risk limits. The final Guidelines do not prescribe the process through which independent risk management reviews and approves policies and risk limits. In some covered banks, independent risk management may be involved from the beginning of the process through the final approval and, in other covered banks, the front line unit may develop risk limits internally and submit them to independent risk management for review, challenge, and approval.

The OCC notes that the standards articulated in paragraphs (b) and (c) of the final Guidelines should not be interpreted as an exclusive list of actions front line units should take to manage risk effectively. Front line units should use their ongoing risk assessments to determine if additional actions are necessary to strengthen risk management practices or reduce risk. For example, there may be instances where front line units should take action to manage risk effectively, even if the covered bank has not exceeded its risk limits.

As described above, the OCC has made revisions to the definition of front line unit that the OCC believes address commenters’ concerns regarding the application of front line unit responsibilities to legal. Several commenters requested clarification on how compliance fits into the risk governance framework and expressed varying views on whether compliance should be considered a front line unit, independent risk management, internal audit, or a different organizational unit. With regard to compliance, the OCC’s guidance is currently outlined in the “Compliance Management System” booklet of the Comptroller’s Handbook and includes responsibilities for all three lines of defense.

Per the Comptroller’s Handbook, a compliance risk management system “includes the compliance program and the compliance audit function.”

The compliance program consists of the policies and procedures which guide employees’ adherence to laws and regulations. Within the Framework, these policies and procedures would generally be the responsibility of the front line unit if they address risks associated with the front line unit’s activities or independent risk management if they address bank-wide or aggregate risks. The Comptroller’s Handbook further states, “[t]he compliance audit function is independent testing of an institution’s transactions to determine its level of compliance with consumer protection laws, as well as the effectiveness of, and adherence with, policies and procedures.”

Within the Framework, the independent testing may be performed by independent risk management, internal audit, or both.

As noted previously, a few commenters asked for additional guidance on the reporting structure for the loan review function. Within the Framework, the loan review function may report to either the second or third line of defense. The loan review function should not report to the executive officer who establishes and oversees front line unit credit policies and individual loan underwriting decisions.

Role and Responsibilities of Independent Risk Management

Independent risk management is the second of a bank’s three lines of defense. Paragraph II.C.2. of the proposed Guidelines provided that independent risk management should oversee the bank’s risk-taking activities and assess risks and issues independent of the CEO and front line units. The proposed Guidelines provided that independent risk management should take primary responsibility and be held accountable by the CEO and board of directors for designing a Framework commensurate with the bank’s size, complexity, and risk profile that meets the Guidelines. Paragraph (b) provided that independent risk management should identify and assess, on an ongoing basis, the bank’s material aggregate risks and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs (c) and (d) of paragraph II.C.2., and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the bank’s risk profile or other conditions. Paragraph (c) provided that independent risk management should establish and adhere to enterprise policies that include concentration risk limits that ensure that aggregate risks within the bank are effectively identified, measured, monitored, and controlled, consistent with the bank’s risk appetite statement and all policies and processes established under paragraphs II.G. through K. Paragraphs (d) and (e) provided that independent risk management should establish and adhere to procedures and processes necessary to ensure compliance with the aforementioned policies and to ensure that the front line units meet the standards discussed in paragraph II.C.1. Paragraph (f) provided that independent risk management should identify and communicate to the CEO and the board of directors or its risk committee material risks and significant instances where independent risk management’s assessment of risk differs.
from a front line unit as well as significant instances where a front line unit is not complying with the Framework. Paragraph (g) provided that independent risk management should identify and communicate to the board of directors or its risk committee material risks and significant instances where independent risk management’s assessment of risk differs from the CEO, and significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the Framework. In addition, the proposed Guidelines provided that independent risk management should develop, attract and retain talent, maintain appropriate staffing levels, and establish and adhere to talent management processes and compensation and performance management programs that comply with paragraphs II.L. and II.M., respectively, of the Guidelines.

Commenters proposed several revisions to this section of the proposed Guidelines. Some commenters requested that the OCC delete the provision discussing independent risk management’s oversight of the bank’s risk-taking activities and assessment of risks and issues independent of the CEO. These commenters expressed concern that this suggested that the CRE would not be subject to CEO oversight with respect to these activities.

Some commenters also noted that including organizational units, such as compliance, legal, and human resources, in the front line unit would require independent risk management to duplicate the control and support functions performed by these other units. These commenters noted that this would detract from independent risk management’s responsibilities for overseeing the risk management program. Other commenters requested that the OCC clarify how independent risk management would interact with organizational units performing control functions. For example, some commenters were concerned that independent risk management’s oversight function would extend to independently assessing the risks imposed by litigation. As described in the section discussing the front line unit definition, the OCC has made revisions to the definition of front line unit that the OCC believes addresses these concerns.

The OCC is finalizing the role and responsibilities of independent risk management substantially as proposed, with several clarifying changes. The OCC has revised the role and responsibilities of independent risk management to remove the provision that independent risk management should assess risks and issues independent of the CEO. The OCC did not intend to suggest that independent risk management should not be subject to CEO oversight with respect to the assessment of risks and issues. Notwithstanding the CEO’s oversight of the CRE and independent risk management, the OCC emphasizes that paragraph (f) of the final Guidelines continues to provide that independent risk management should report to the board of directors or its risk committee material risks and significant instances where independent risk management’s assessment of risk differs from the CEO, as well as significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the Framework.

The OCC also emphasizes that the standards articulated in paragraphs (c) and (d) of the final Guidelines should not be interpreted as an exclusive list of actions independent risk management should take to effectively manage risk. Independent risk management should use its risk assessments to determine if additional actions are necessary to strengthen risk management practices or reduce risk. For example, there may be instances where independent risk management should take action to effectively manage risk, even if the covered bank’s risk appetite, applicable concentration risk limits, or a front line unit’s risk limits have not been exceeded.

The OCC also has removed paragraph (e), and redesignated paragraph (f) as new paragraph (e). The OCC has revised new paragraph (e) to clarify that independent risk management should identify and communicate to the CEO and the board of directors, or the risk committee, significant instances where a front line unit is not adhering to the Framework, including instances when front line units do not meet the standards set forth in paragraph II.C.1.

Role and Responsibilities of Internal Audit

Internal audit is the third of a bank’s three lines of defense. The proposed Guidelines provided that internal audit should ensure that a bank’s Framework complies with the Guidelines and is appropriate for the bank’s size, complexity, and risk profile. Paragraph (a) provided that internal audit should maintain a complete and current inventory of all of the bank’s material businesses, product lines, services, and functions and assess the risks associated with each, which collectively provide a basis for the audit plan.

Paragraph (b) provided that internal audit should establish and adhere to an audit plan updated at least quarterly that takes into account the bank’s risk profile as well as emerging risks and issues. The proposal provided that the audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and independent risk management under the Framework. The proposal provided that changes to the audit plan should be communicated to the audit committee of the board of directors.

Paragraph (c) provided that internal audit should report to the audit committee conclusions, issues, and recommendations resulting from the audit work carried out under the audit plan. These reports should identify the root cause of any issue and include a determination of whether the root cause creates an issue that has an impact on one organizational unit or multiple organizational units within the bank, as well as a determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner.

Paragraph (d) provided that internal audit should establish and adhere to processes for independently assessing the design and effectiveness of the Framework. The assessment should be performed at least annually and may be conducted by internal audit, an external party, or a combination of both. The assessment should include a conclusion on the bank’s compliance with the Guidelines and the degree to which the bank’s Framework is consistent with leading industry practices.

Paragraph (e) provided that internal audit should identify and communicate to the audit committee significant instances where front line units or independent risk management are not adhering to the Framework. Paragraph (f) provided that internal audit should establish a quality assurance department.
that ensures internal audit’s policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the bank, are updated to reflect changes to internal and external risk factors, and are consistently followed. Finally, the proposed Guidelines provided that internal audit should develop, attract, and retain talent and maintain appropriate staffing levels, and establish and adhere to talent management processes and compensation and performance management programs that comply with paragraphs I.II. and I.I.M., respectively, of the proposed Guidelines.

The OCC invited comment as to whether the final Guidelines should provide that independent risk management maintain a complete and current inventory of all of a bank’s material businesses, product lines, services, and functions to ensure that internal audit has developed an accurate inventory. The OCC also requested comment on whether internal audit’s assessment of the bank’s Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. The OCC inquired as to whether such an assessment would be possible given the wide range of industry practices, and whether there were any concerns related to this provision.

Commenters generally stated that the role and responsibilities assigned to internal audit were too prescriptive. Some commenters requested that the final Guidelines provide that internal audit report to the audit committee only on material changes to the audit plan, material audit findings and conclusions, and root causes of material audit matters. Other commenters noted that internal audit may not need to assess the Framework’s design annually since the design of the Framework is not likely to materially change on a frequent basis. These commenters also expressed concern that the proposed Guidelines could permit an external party to assess the Framework, and requested that the final Guidelines clarify that internal audit must oversee the external party. Some commenters also argued that it is not necessary for internal audit to establish a quality assurance department because this is already a function of internal audit.

Commenters also requested clarification regarding a discussion in the preamble to the proposed Guidelines providing, in part, that the audit plan should derive the risk presented by each front line unit, product line, service, and function, and that internal audit should derive these ratings from bank-wide risk assessments. Some commenters requested clarification regarding whether the bank-wide risk assessments are prepared by internal audit independently, or whether these assessments are prepared by internal audit in conjunction with front line units and/or independent risk management. Other commenters suggested that permitting internal audit to periodically adjust these ratings based on risk assessments conducted by front line units may compromise internal audit’s independence and objectivity. Some commenters suggested that internal audit should conduct an independent assessment, and provide challenges where appropriate, to the risk assessments conducted by front line units.

Commenters disagreed whether both independent risk management and internal audit should maintain a complete and current inventory of all of a bank’s material businesses, product lines, services, and functions. Some commenters argued that front line units should be responsible for this inventory, rather than internal audit. Other commenters asserted that independent risk management should maintain this inventory rather than internal audit. These commenters noted that internal audit should review and evaluate the inventory for accuracy and completeness if it is maintained by independent risk management. Other commenters expressed the view that banks should have flexibility in determining which inventory, whether independent risk management or internal audit is responsible for maintaining the inventory. These commenters emphasized that banks should only be required to maintain one comprehensive inventory, and that front line units should play a significant role in the creation of the inventory.

The majority of commenters also opposed the proposed Guidelines to the extent they provided that internal audit’s assessment of the bank’s Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. Some commenters noted that this would be a subjective determination as there is no basis for determining what constitutes leading industry practices, and argued that this may lead covered banks to make greater operational burdens on the audit process. Other commenters argued that internal audit should report discrepancies in the creation of the inventory. The OCC expects internal audit to leverage risk assessments conducted by front line units or independent risk management in deriving the risk assessments discussed in paragraph (a), but should apply independent judgment in doing so. Internal audit may periodically adjust its risk assessments based on changes in the covered bank’s strategy and the external environment. The audit plan should include ongoing monitoring to identify emerging risks and ensure that units, product lines, services, and functions that receive a low risk rating are reevaluated with reasonable frequency.

The OCC’s final Guidelines contain revisions to address some of the concerns raised by commenters and provide internal audit more flexibility in satisfying its role and responsibilities under the Framework. For example, the OCC agrees with commenter suggestions that internal audit should report conclusions and material issues and recommendations to the audit committee pursuant to paragraph (c), and that such reports should also identify the root cause of any material issues. The OCC believes that this modification avoids imposing undue operational burdens on the audit committee and enables the committee to fulfill its key oversight role.

The OCC believes that the design and implementation of the audit plan is an important element of internal audit’s role and responsibilities under the Framework. The inventory of material processes, product lines, services, and functions and the risk assessments conducted by internal audit pursuant to paragraph (a) of the final Guidelines is commonly referred to as the “internal audit universe” and forms the basis of the audit plan. The OCC expects internal audit to conduct these risk assessments independent of other organizational units in the covered bank. As explained in the preamble to the proposed Guidelines, the audit plan should rate the risk presented by each front line unit, product line, service, and function. This includes activities that the covered bank may outsource to a third party.

Internal audit can leverage risk assessments conducted by front line units or independent risk management in deriving the risk assessments discussed in paragraph (a), but should apply independent judgment in doing so. Internal audit may periodically adjust its risk assessments based on changes in the covered bank’s strategy and the external environment. The audit plan should include ongoing monitoring to identify emerging risks and ensure that units, product lines, services, and functions that receive a low risk rating are reevaluated with reasonable frequency.

44 The OCC does not believe that permitting internal audit to leverage risk assessments conducted by front line units or independent risk management compromises internal audit’s independence or objectivity. Specifically, the OCC expects internal audit to report discrepancies in internal audit’s risk ratings and a front line unit’s or independent risk management’s risk ratings to the audit committee of the board of directors.
The audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and independent risk management under the Framework. The OCC notes that this provision is in addition to internal audit’s traditional testing of internal controls and the accuracy of financial records, as required by other laws and regulations at an appropriate frequency based on risk. This testing should ensure the evaluation of reputation and strategic risk, along with evaluations of independent risk management and traditional risks. This testing should enable internal audit to assess the appropriateness of risk levels and trends across the covered bank.

Consistent with the proposal, the OCC continues to believe that all significant changes to the audit plan should be communicated to the audit committee. As discussed earlier, the OCC believes that the audit plan is a critical element of internal audit’s role and responsibilities under the Framework and that significant changes to the audit plan are material. The final Guidelines also clarify that internal audit should periodically review and update the audit plan, rather than performing this task on a quarterly basis as provided in the proposed Guidelines.

Paragraph (c) provides, in part, that internal audit should report in writing, conclusions and material issues and recommendations resulting from audit work carried out under the audit plan. The OCC also notes that these reports should include potential and emerging concerns, the timeliness of corrective actions, and the status of outstanding issues. Finally, audit reports should include comments on the effectiveness of front line units and independent risk management in identifying and mitigating excessive risks and identifying and resolving issues in a timely manner. Audit reports should also reflect emerging risks and internal audit’s assessment of the appropriateness of risk levels relative to both the quality of the internal controls and the risk appetite statement.

The OCC has also clarified the role and responsibilities of internal audit under the final Guidelines. Specifically, the final Guidelines provide that internal audit should assess emerging risks and that the quality assurance program should ensure that internal audit’s policies, procedures, and processes are updated to reflect emerging risks and improvements in industry internal audit practices. The addition of emerging risks is intended to emphasize that internal audit should consider both pre-existing and prospective risks with respect to the relevant provisions. The OCC also believes that those individuals carrying out the quality assurance program should remain apprised of evolving industry internal audit practices, and that internal audit’s policies, procedures, and processes should be updated to reflect these improved practices, as appropriate. The OCC has not removed the provision regarding the establishment of a quality assurance program, as one commenter suggested, because the OCC’s supervisory experience indicates that all covered banks’ internal audit units include a quality assurance function.

The OCC has made important revisions to internal audit’s role and responsibilities for assessing the design and ongoing effectiveness of the Framework. The final Guidelines continue to provide that this assessment should be conducted at least annually because there may be situations (e.g., expansion of business, change in strategy, emerging risks) that cause the covered bank’s risk profile to change, thereby justifying a reassessment of the design and ongoing effectiveness of the covered bank’s Framework. The final Guidelines also continue to provide that internal audit, an external party, or both may perform this assessment. The OCC has not revised the final Guidelines to provide that internal audit must oversee this external party. The OCC notes that there may be situations where a covered bank wants to engage a third party to review the entire Framework, including internal audit’s role in the Framework. It would not be appropriate for internal audit to oversee the external party in this situation. In addition, based on the overwhelming majority of comments, the OCC is modifying this paragraph to remove the provision that internal audit’s assessment of the Framework should include a conclusion regarding whether the Framework is consistent with leading industry practices. However, the OCC notes that most covered banks that experienced difficulties during the financial crisis had risk management that were not commensurate with the scope of the covered bank’s business activities. As a result, the OCC expects independent risk management, in conjunction with internal audit, the CEO, and the board of directors to assess whether the covered bank’s risk management practices are developing in an appropriate manner and consider benchmarking these practices against peers, where possible.

The final Guidelines continue to provide that internal audit should maintain a complete and current inventory (“audit universe”) of all of the covered bank’s material processes, product lines, services, and functions. The OCC agrees with commenter suggestions that a covered bank should only be required to maintain one inventory. The OCC believes that internal audit should maintain this inventory, because it is a key component in the creation of the audit plan. Front line units and independent risk management are expected to conduct risk assessments as part of their responsibilities within the Framework and internal audit may use these risk assessments when conducting its risk assessment against the inventory.

**Stature**

As we noted in the preamble to the proposal, a critical part of an effective Framework is for independent risk management and internal audit to have the organizational stature needed to effectively carry out their respective roles and responsibilities. One of the primary reasons for assigning CRE and CAE responsibilities to individuals who report directly to the CEO is to establish organizational stature for these units. However, evidence of stature extends beyond the reporting structure. Appropriate stature is evidenced by the attitudes and level of support provided by the board of directors, CEO, and others within the covered bank toward these units. The board of directors demonstrates support for these units by ensuring that they have the resources needed to carry out their responsibilities and by relying on the work of these units when carrying out their oversight responsibilities set forth in section III of the final Guidelines. The CEO and front line units demonstrate support by welcoming credible challenges from independent risk management and internal audit and including these units in policy development, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes.

**Strategic Plan**

Paragraph D. of section II of the proposed Guidelines provided that the CEO should develop a written strategic plan with input from front line units and independent risk management. The proposal also provided that the board of directors should evaluate and approve the strategic plan and monitor management’s efforts to implement it at least annually. Under the proposed Guidelines the strategic plan would cover a three-year period and would contain a comprehensive assessment of risks that currently have an impact on the bank or that could have an impact
on the bank during this period, articulate an overall mission statement and strategic objectives for the bank, and include an explanation of how the bank will achieve those objectives.

The proposal also provided that the strategic plan should include an explanation of how the bank will update the Framework and account for changes in the bank’s risk profile projected under the strategic plan. Finally, the proposed Guidelines required the bank to review, update and approve the strategic plan due to changes in the bank’s risk profile or operating environment that were not contemplated when the plan was developed.

Some commenters suggested that the CEO should “oversee” rather than “develop” the strategic plan. Other commenters recommended that the OCC require “material” risks to be included in the comprehensive assessment of risks. One commenter suggested that the strategic plan incorporate a capital plan. Some commenters objected to the requirement that the plan include an explanation of how the bank will update the Framework to account for changes in the bank’s risk profile. The commenters argued that annual review was sufficient. Another commenter argued that internal audit should not be included in the development of the strategic plan since its involvement could compromise the independence of internal audit.

The OCC is adopting this paragraph substantially as proposed with one minor revision. We have changed the language in the final Guidelines so that a CEO should be “responsible for the development of,” rather than “develop,” a written strategic plan. This change clarifies that a CEO is not individually expected to prepare the strategic plan. The final Guidelines do not include a materiality threshold for what risks covered banks must assess. While the OCC understands that certain de minimis risks may be excluded from the risk assessment, the strategic plan should comprehensively assess all risks that could reasonably be expected to have an impact on the covered bank.

The final Guidelines, like the proposed Guidelines, require a three-year plan. The OCC believes that a three-year plan is necessary for covered banks to predict changes that could affect the bank’s financial position. If a covered bank experiences, or expects to experience, significant changes over a three-year time horizon, it must be able to predict and manage the risks associated with those changes. A strategic plan of less than three years would be insufficient to manage longer-term risks to the covered bank. The final Guidelines also do not include a requirement for a specific capital plan. While the OCC acknowledges the importance of capital planning, the final Guidelines are focused on risk management rather than on ensuring adequate capital ratios.

The board of directors should evaluate and approve the strategic plan and monitor management’s efforts to implement the strategic plan at least annually. While the OCC expects that for some covered banks an annual review of the Framework may be sufficient, other covered banks that have undergone major changes (for example, mergers) are expected to update their Frameworks to account for changed circumstances. The final Guidelines, like the proposal, provide that the strategic plan should be developed with input from internal audit. The OCC believes that internal audit can contribute to a strategic plan while maintaining the appropriate level of independence.

Risk Appetite Statement

Paragraph E. of section II of the proposed Guidelines provided that the bank should have a comprehensive written statement that articulates a bank’s risk appetite and serves as a basis for the Framework (Statement). The term risk appetite means the aggregate level and types of risk the board and management are willing to assume to achieve the bank’s strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements.

The proposal noted that the Statement should include: (i) Qualitative components that describe a safe and sound “risk culture” and how the bank would assess and accept risks, including those that are difficult to quantify; and (ii) quantitative limits that incorporate sound stress testing processes and, as appropriate, address the bank’s earnings, capital and liquidity position. The proposed Guidelines also provided that the bank should set limits at levels that consider applicable capital, liquidity, and internal audit. The proposed Guidelines required that the bank’s risk profile jeopardizes the adequacy of its earnings, capital, and liquidity. The proposed Guidelines also required that the bank’s risk profile jeopardizes the adequacy of its earnings, capital, and liquidity.

One commenter objected to the language in the preamble to the proposed Guidelines providing that when a bank’s risk profile is substantially the same as its parent company, the bank’s board may tailor the parent company’s risk appetite statement to make it applicable to the bank. According to the commenter, a bank that meets the “substantially the same” test should be able to use the same risk appetite statement as its parent company. Another commenter requested clarification on the extent to which the board of directors is required to approve risk limits in connection with a Statement. The commenter argued that bank directors are not in a position to approve all of the limits necessary to manage risk.

The OCC is adopting this paragraph as proposed with only technical changes. As with the proposed Guidelines, the final Guidelines do not include a specific regulatory definition of risk culture. However, setting an appropriate tone at the top is critical to establishing a sound risk culture, and the qualitative statements within the Statement should articulate the core values that the board and CEO expect employees throughout the covered bank to share when carrying out their respective roles and responsibilities within the covered bank. These values should serve as the basis for risk-taking decisions made throughout the covered bank and should be reinforced by the actions of the board, executive management, board committees, and individuals. As noted in the preamble to the proposed Guidelines, evidence of a sound risk culture includes, but is not limited to: (i) Open dialogue and transparent sharing of information between front line units, independent risk management, and internal audit; (ii) consideration of all relevant risks and the views of independent risk management and internal audit; and (iii) clear performance management programs and decisions that reward compliance with the core values and quantitative limits established in the Statement, and hold accountable those who do not conduct themselves in a manner consistent with these articulated standards.

As described in paragraph I.E. of the final Guidelines, quantitative limits in a covered bank’s Statement should

45 While there is no regulatory definition of risk culture, for purposes of these Guidelines, risk culture can be considered the shared values, attitudes, competencies, and behaviors present throughout the covered bank that shape and influence governance practices and risk decisions.

46 The term and types of risk covered bank management and the board of directors are willing to assume to achieve the bank’s strategic objectives and business plan should be consistent with its capital and liquidity needs and requirements, as well as other laws and regulatory requirements applicable to the covered bank. The board is not responsible for setting specific risk limits, but the board is required to review and approve the Statement.
incorporate sound stress testing processes, as appropriate, and should address the covered bank’s earnings, capital, and liquidity. The covered bank may set quantitative limits on a gross or net basis. Lagging indicators, such as delinquencies, problem asset levels, and losses generally will not capture the build-up of risk during healthy economic periods. As a result, these indicators are generally not useful in proactively managing risk. However, setting quantitative limits based on performance under various adverse scenarios would enable the board and management to take actions that reduce risk before delinquencies, problem assets, and losses reach excessive levels.

We expect examiners to apply judgment when determining which quantitative limits should be based on stress testing and to consider several factors, including, for example, the value in using such measures for the risk type, the covered bank’s ability to produce such measures, the capabilities of similarly-situated institutions, and the degree to which the covered bank’s board and management have invested in the resources needed to establish such capabilities. We note that the Federal banking agencies issued guidance on stress testing in May 2012.\(^4\) The guidance describes various stress testing approaches and applications, and covered banks should consider the range of approaches and select the one(s) most suitable when establishing quantitative limits. Risk limits may be designed as thresholds, triggers, or hard limits, depending on how the board and management choose to manage risk. Thresholds or triggers that prompt discussion and action before a hard limit is reached or breached can be useful tools for reinforcing risk appetite and proactively responding to elevated risk indicators.

When a covered bank’s risk profile is substantially the same as that of its parent company, the covered bank’s board may tailor the parent company’s risk appetite statement to make it applicable to the covered bank. However, to ensure the sanctity of the national bank or Federal savings association charter, the board of any covered bank must approve the bank-level Statement and document any necessary adjustments or material differences between the covered bank’s and parent company’s risk profiles.

Concentration and Front Line Unit Risk Limits

Paragraph F. of section II of the proposed Guidelines provided that the Framework should include concentration risk limits and, as applicable, front line unit risk limits for the relevant risks in each front line unit to ensure that these units do not create excessive risks. The proposal also provided that when aggregated across units, these risks do not exceed the limits established in the bank’s risk appetite statement.

One commenter suggested that the word “ensure” should not be used in this paragraph as it implies a guaranteed outcome. The commenter suggested a slightly different formulation of the language in this paragraph. The OCC is adopting this paragraph as proposed with the addition of the commenter’s suggestion. The final Guidelines, state that concentration and front line unit risk limits should limit excessive risk taking.

Risk Appetite Review, Monitoring, and Communication Processes

Paragraph G. of section II of the proposed Guidelines provided that the Framework should require: (i) Review and approval of the Statement by the board or the board’s risk committee at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the bank’s business model, strategy, risk profile, or market conditions; (ii) initial communication and ongoing reinforcement of the bank’s Statement throughout the bank to ensure that all employees align their risk-taking decisions with the Statement; (iii) independent risk management to monitor the bank’s risk profile in relation to its risk appetite and compliance with concentration risk limits and to report such monitoring to the board or the board’s risk committee at least quarterly; (iv) front line units to monitor their respective risk limits and to report to independent risk management at least quarterly; and (v) when necessary due to the level and type of risk, independent risk management to monitor front line units’ compliance with front line unit risk limits, ongoing communication with front line units regarding adherence to these risk limits, and to report any concerns to the CEO and the board or the board’s risk committee, at least quarterly.

We received only minor comments on this paragraph and, accordingly, we are adopting paragraph G. of the final Guidelines substantially as proposed, with a few technical changes. With regard to the monitoring and reporting set forth in paragraph G., we note that the frequency of such monitoring and reporting should be performed more often, as necessary, based on the size and volatility of the risks and any material change in the covered bank’s business model, strategy, risk profile, or market conditions.

Processes Governing Risk Limit Breaches

Paragraph H. of section II of the proposed Guidelines set out processes governing risk limit breaches. The proposal provided that the bank should establish and adhere to processes that require front line units and independent risk management, in conjunction with their respective responsibilities, to identify any breaches of the Statement, concentration risk limits, and front line unit risk limits, distinguish identified breaches based on the severity of their impact on the bank and establish protocols for when and how to inform the board, front line management, independent risk management, and the OCC of these breaches. The proposed Guidelines also provided that the bank should include in the protocols discussed above the requirement to provide a written description of how a breach will be, or has been, resolved and establish accountability for reporting and resolving breaches that include consequences for risk limit breaches that take into account the magnitude, frequency, and recurrence of breaches. Under the proposal, while both escalation and resolution processes are important elements of the Framework, it would be acceptable for banks to have different escalation and resolution processes for breaches of the Statement, concentration risk limits, and front line unit risk limits.

The OCC did not receive any comments on this paragraph, and is adopting it as proposed with one change. We have included internal audit in the list of groups that will be informed of a risk limit breach.

Concentration Risk Management

Paragraph I. of section II of the proposed Guidelines provided that the Framework should include policies and supporting processes that are appropriate for the bank’s size, complexity, and risk profile that effectively identify, measure, monitor, and control the bank’s concentration of risk. The OCC received no comments on this paragraph, and the final Guidelines are adopted as proposed with minor technical changes.

Concentrations of risk can arise in any risk category, with the most common being identified with borrowers, funds providers, and counterparties. In addition, the OCC’s eight categories of risk discussed earlier are not mutually

\(^4\) 77 FR 29458 (May 17, 2012).
exclusive; any product or service may expose a covered bank to multiple risks and risks may also be interdependent.\(^48\) Furthermore, concentrations can exist on and off the balance sheet. Covered banks should continually enhance their concentration risk management processes to strengthen their ability to effectively identify, measure, monitor, and control concentrations that arise in all risk categories.\(^49\)

Risk Data Aggregation and Reporting

Paragraph J. of section II of the proposed Guidelines addressed risk data aggregation and reporting. This paragraph provided that the Framework should include a set of policies, supported by appropriate procedures and processes, designed so that the bank’s risk data aggregation and reporting capabilities are appropriate for its size, complexity, and risk profile and support supervisory reporting requirements. The proposal provided that these policies, procedures, and processes should collectively provide for the design, implementation, and maintenance of data architecture and information technology infrastructure that support the bank’s risk aggregation and reporting needs in times of normalcy and 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 and the distribution of risk reports to all relevant parties at a frequency that meets the needs for decision-making purposes.

The OCC is adopting the final Guidelines substantially as proposed with a few technical changes. The OCC expects covered banks to have risk aggregation and reporting capabilities that meet the board’s and management’s needs for proactively managing risk and ensuring the covered bank’s risk profile remains consistent with its risk appetite.

Relationship of Risk Appetite Statement, Concentration Risk Limits, and Front Line Unit Risk Limits to Other Processes

Paragraph K. of section II of the proposed Guidelines addressed the relationship between the Statement, concentration risk limits, and front line unit risk limits to other bank processes. The OCC received no comments on this paragraph and the OCC is adopting this section as proposed with minor

date: \(48\) See “Large Bank Supervision” booklet of the Comptroller’s Handbook (Jan. 2010).

\(^{49}\) See “Concentrations of Credit” booklet of the Comptroller’s Handbook (Dec. 2011); Interagency Supervisory Guidance on Counterparty Credit Risk Management at http://www.occ.gov/news-issuances/bulletin/2011/bulletin-2011-30.html. technical changes. The covered bank’s front line units and independent risk management should incorporate at a minimum the Statement, concentration risk limits, and front line unit risk limits into their strategic and annual operating plans, capital stress testing and planning processes, liquidity stress testing and planning processes, product and service risk management processes (including those for approving new and modified products and services), decisions regarding acquisitions and divestitures, and compensation performance management programs.

Talent Management Processes

The proposed Guidelines provided that the bank should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. This paragraph also provided that a bank’s talent management processes should ensure that the board of directors or a committee of the board: (i) hires a CEO and approves the hiring of direct reports of the CEO with the skills and abilities to design and implement an effective Framework; (ii) establishes reliable succession plans for the CEO and his or her direct reports; and (iii) oversees the talent development, recruitment, and succession planning processes for individuals two levels down from the CEO. The proposal also provided that these processes should ensure that the board of directors or a committee of the board: (i) hires one or more CREs and a CAE that possess the skills and abilities to effectively implement the Framework; (ii) establishes reliable succession plans for the CRE and CAE; and (iii) oversees the talent development, recruitment, and succession planning processes for independent risk management and internal audit.

Some commenters asserted that these provisions would impose administrative burdens on a bank’s board of directors and inappropriately place operational management responsibilities on the board. Commenters noted that the establishment of succession plans for direct reports of the CEO and the oversight of talent development, recruitment, and succession processes for independent risk management, internal audit, and individuals two levels down from the CEO would be burdensome and are more appropriately assigned to bank management. These commenters argued that the OCC should remove these provisions from the final Guidelines.

One commenter noted that it would be sufficient for the board of directors to oversee the talent development, recruitment, and succession planning for individuals one level down from the CEO. Another commenter argued that the OCC should expressly require succession planning for individuals two levels down from the CRE and CAE and require that succession plans identify one or more viable candidates for key positions. Another commenter construed this paragraph as imposing a general requirement that all banks hire dedicated CEOs, CREs, and CAEs, and argued that banks should be permitted to rely on “dual-hatted” employees. As previously discussed, the final Guidelines permit a covered bank to use components of its parent company’s risk governance framework, including having employees serve in the same position at the covered bank and the parent company, to the extent this is appropriate for the covered bank. The OCC believes that this responds to this commenter’s concerns.

In light of the comments received, the OCC has revised this paragraph to reduce the operational burdens on the board of directors while maintaining appropriate board oversight of the talent management program for employees with significant responsibilities under the Framework. The final Guidelines provide that a covered bank’s board of directors or an appropriate committee of the board should appoint a CEO and one or more CREs with the skills and abilities to carry out their roles and responsibilities within the Framework. This provision clarifies that the board of directors need not be involved in the hiring process for these individuals. This gives the board, or a committee thereof, the option to rely on management to appoint the CAE and CRE(s).\(^50\) Similarly, the final Guidelines provide that a covered bank’s board of directors or an appropriate committee of the board should review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the CEO, CAE, CRE(s), their direct reports, and other potential successors. The OCC

\(^{50}\) The OCC notes that the definition of “independent risk management” provides that the board of directors or its risk committee should approve all decisions regarding the appointment or removal of a CRE, while the definition of “internal audit” provides that the audit committee should approve all decisions regarding the appointment or removal of the CAE. See final Guidelines paragraphs 1.E.7. and 8.
believes that this revision reduces the talent management responsibilities of the board of directors, or a committee thereof, because they are no longer expected to oversee the talent development, recruitment, and succession planning processes for independent risk management, internal audit, and individuals two levels down from the CEO, as provided in the proposed Guidelines. Instead, the board of directors, or a committee thereof, should review and approve a written talent management program for key employees in a covered bank’s Framework. The OCC notes that it is very important that covered banks detail the development, recruitment, and succession planning for these individuals because they occupy critical positions in a covered bank’s Framework.

Finally, the final Guidelines provide that a covered bank’s board of directors or an appropriate committee of the board should require management to assign individuals specific responsibilities within the talent management program, and hold those individuals accountable for the program’s effectiveness. This provision clarifies that the OCC expects the board of directors, or a committee thereof, to provide oversight to a covered bank’s talent management program, and that responsibility for developing and implementing this program rests with covered bank management.

Compensation and Performance Management Programs

The proposed Guidelines provided that a bank should establish and adhere to compensation and performance management programs that meet the requirements of any applicable statute or regulation. The proposal provided that these programs should be appropriate to ensure that the CEO, front line units, independent risk management, and internal audit implement and adhere to an effective Framework. The proposal also provided that programs should ensure that front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit. The programs should be designed to attract and retain the talent needed to design, implement, and maintain an effective Framework. Finally, the proposed Guidelines provided that the programs should prohibit incentive-based payment arrangements, or any feature of any such arrangement, that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

Some commenters supported this paragraph of the proposed Guidelines. One commenter argued that employee compensation should be linked to the entire organization’s strategic goals and should incorporate organization-wide performance metrics. Another commenter requested that the OCC provide more specific standards for compensation. A commenter also objected to the proposed Guidelines to the extent they provided that the programs should ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues, and instead suggested that the Guidelines should emphasize the timely correction of issues. Commenters also disagreed regarding the inclusion of the incentive compensation provision in the proposed Guidelines. Some commenters suggested that the proposed Guidelines should contain stronger language prohibiting incentive-based payment arrangements that encourage inappropriate risk. Other commenters argued that one could interpret this provision as creating standards beyond those established by existing interagency guidance as well as those set out in joint agency proposed rulemaking. These commenters recommended revising this provision to state that a bank’s compensation and performance management programs should meet the requirements of applicable laws and regulations.

After reviewing the comments received, the OCC is adopting the compensation and performance management program paragraph substantially as proposed with clarifying and technical changes. The OCC has revised this paragraph to provide that the compensation and performance management programs should ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit, as well as the timeliness of corrective action to resolve such issues and concerns. The OCC declines to remove the term “severity,” as suggested by one commenter because we believe this is an important factor in determining the materiality of issues and concerns. The OCC also has decided not to modify the remaining provisions of this paragraph, including the incentive compensation standard. As previously discussed, the final Guidelines establish minimum standards for the design and implementation of a covered bank’s Framework and minimum standards for the covered bank’s board of directors in providing oversight to the Framework’s design and implementation. While compensation practices are an important part of a covered bank’s Framework, the OCC notes that other authorities address this issue in more detail.

The OCC reminds covered banks that employee compensation arrangements should comply with all applicable rules and guidance. The OCC also notes that section 956 of the Dodd-Frank Act requires the OCC, the Board, the FDIC, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Housing Finance Agency to jointly prescribe incentive-based regulations or guidelines applicable to covered institutions. The OCC notes that the incentive compensation standard included in the final Guidelines was adapted from the standard set out in section 956 of the Dodd-Frank Act, and that a covered bank’s compensation and performance management programs should comply with the final regulations or guidelines implementing section 956 when they are issued.

Section III: Standards for Board of Directors

Section III of the final Guidelines sets forth the minimum standards for a covered bank’s board of directors in providing oversight to the Framework’s design and implementation.

Some commenters expressed concern regarding the standards contained in section III of the proposed Guidelines. For example, some commenters argued that the proposed Guidelines would distract the board of directors from its strategic and oversight role. Other commenters asserted that the proposed Guidelines would place an undue burden on the board of directors by assigning managerial responsibilities to the board that are more properly the role of:

51 See 12 U.S.C. 1831p–1(c); 12 CFR part 30, Appendix A (requiring institutions to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to an institution, and prohibiting excessive compensation as an unsafe and unsound practice). As provided in the Guidelines, covered banks subject to the final Guidelines should ensure that practices established within their Frameworks also meet the standards set forth in appendices A, B, and C to part 30. See final Guidelines II.C. note 2. We also note that the OCC, Board, the Federal Deposit Insurance Corporation (FDIC), and the OTS issued interagency guidance that addresses incentive-based compensation. See Guidance on Sound Incentive Compensation Policies, 75 FR 36395 (June 25, 2010).


of bank management. Some commenters also argued that the oversight mandated by the proposed Guidelines would increase a board of directors’ exposure to liability and discourage qualified individuals from agreeing to serve on the board.

The OCC has revised the standards to recognize the board of directors’ key strategic and oversight role with respect to the design and implementation of the Framework. The OCC believes that these revisions respond to commenters’ concerns and avoid imposing an undue operational burden on the board of directors. Set forth below is a discussion of the minimum standards for a covered bank’s board of directors in providing oversight to the Framework’s design and implementation under the final Guidelines.

Require an Effective Risk Governance Framework

Paragraph A. of section III of the proposed Guidelines provided that each member of the bank’s board of directors has a duty to oversee the bank’s compliance with safe and sound banking practices. The proposed Guidelines also provided that the board of directors or its risk committee should approve any changes to the Framework.

Many commenters strongly opposed the use of the word “ensure” in the proposed Guidelines. Some commenters noted that the term “ensure” could be read as a guarantee of results and understood to imply that the board of directors is required to be involved in the day-to-day activities of the bank. These commenters asserted that it may make it more difficult for banks to attract qualified candidates for a bank’s board of directors and may imply that the board could be held liable for management actions even when director oversight has been reasonable. Other commenters suggested that the final Guidelines should provide that a board of directors fulfills its oversight function by reviewing, evaluating, and approving a Framework that is designed, recommended, and implemented by management and by receiving reports on material compliance matters.

Many commenters recommended that the OCC remove the word “ensure” from the final Guidelines, and provided a number of alternatives to address their concerns. Commenters suggested that the OCC replace “ensure” with “Require,” “oversee,” “actively oversee,” and “oversee and confirm.” Commenters generally argued that these alternatives more accurately reflect the board of directors’ oversight function.

After reviewing the comments, the OCC is revising this paragraph of the final Guidelines to remove the terms “duty” and “ensure.” The OCC did not intend to impose managerial responsibilities on the board of directors, or suggest that the board must guarantee results under the Framework. Accordingly, consistent with commenter suggestions, the final Guidelines provide that the board of directors should require management to establish and implement an effective Framework that meets the minimum standards described in the Guidelines. The OCC believes that this revision aligns the board of directors’ responsibilities under this paragraph with their traditional strategic and oversight role.

The OCC has also modified this paragraph to reduce the operational burdens placed on the board of directors while maintaining their involvement in overseeing the Framework’s design and implementation. The final Guidelines clarify that the board of directors or its risk committee should approve significant changes to the Framework and monitor compliance with the Framework. The revision clarifies that the board or risk committee should only approve significant changes to the Framework, rather than all changes, as provided in the proposed Guidelines. This change also clarifies that the board of directors or the risk committee should monitor compliance with the Framework by overseeing management’s implementation of the Framework and holding management accountable for fulfilling their responsibilities under the Framework.

Provide Active Oversight of Management

Paragraph B. of section III of the proposed Guidelines provided that the board of directors should actively oversee the bank’s risk-taking activities and hold management accountable for adhering to the Framework.

The OCC believes that the capacity to provide a credible challenge to management—instead, the board is permitted to rely on independent risk management and internal audit to meet its responsibilities under this paragraph. Some boards of directors periodically engage third-party experts to assist them in understanding risks and issues and to make recommendations to strengthen board and bank practices. While the Guidelines focus on independent risk management and internal audit, they do not prohibit boards of directors from engaging third-party experts to also assist them in carrying out their duties.

The final Guidelines continue to articulate the OCC’s expectation that the board of directors should provide a credible challenge to management. The OCC believes that a board of directors will be able to provide this challenge if its members have a comprehensive understanding of the covered bank’s risk-taking activities. During the financial crisis, the OCC observed that some members of the board of directors at certain institutions had an incomplete understanding of their institution’s risk exposures. The OCC believes that this evidences both a failure to exercise adequate oversight of management and critically evaluate management’s recommendations and decisions during the years preceding the financial crisis. The OCC believes that the capacity to engage, monitor, and oversee management is critical in order to effectively fulfill the OCC’s responsibilities in overseeing risk-taking activities and ensuring the safety and soundness of the covered bank. The OCC believes that the proposed Guidelines strike an appropriate balance between the OCC’s responsibilities in overseeing the board of directors and bank management’s responsibilities under the Framework. The OCC believes that it is important for the board of directors to understand a covered bank’s risk-taking activities and to be engaged in providing oversight to these activities. The final Guidelines clarify that the board of directors provides active oversight by relying on risk assessments and reports prepared by independent risk management and internal audit. Therefore, the final Guidelines do not contemplate that the board of directors will assume managerial responsibilities in providing active oversight of management—instead, the board is permitted to rely on independent risk management and internal audit to meet its responsibilities under this paragraph. Some boards of directors periodically engage third-party experts to assist them in understanding risks and issues and to make recommendations to strengthen board and bank practices. While the Guidelines focus on independent risk management and internal audit, they do not prohibit boards of directors from engaging third-party experts to also assist them in carrying out their duties.
reviewing information and developing an understanding of the key issues related to a covered bank’s risk-taking activities is a critical prerequisite to being an effective director. Informed directors are well-positioned to engage in substantive discussions with management wherein the board of directors provides approval to management, requests guidance to clarify areas of uncertainty, and prudently questions the propriety of strategic initiatives. Therefore, the final Guidelines continue to provide that the board of directors, in reliance on information it receives from independent risk management and internal audit, should 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. In addition to resulting in a more informed board of directors, the OCC expects that this provision will enable the board to make a determination as to whether management is adhering to, and understands, the Framework. For example, recurring breaches of risk limits or actions that cause the covered bank’s risk profile to materially exceed its risk appetite may demonstrate that management does not understand or is not adhering to the Framework. In these situations, the board of directors should take action to hold the appropriate party, or parties, accountable.

The OCC does not intend this standard to become a compliance exercise for the covered bank, or lead to scripted meetings between the board of directors and management. Instead, the OCC intends to assess compliance with this standard primarily by engaging OCC examiners in frequent conversations with directors. Likewise, the OCC does not expect the board of directors to evidence opposition to management during each board meeting. Instead, the OCC emphasizes that the board of directors should oppose management’s recommendations and decisions only when necessary. The OCC believes that an environment in which examiners, board members, and management openly and honestly communicate benefits a covered bank, and expects these types of interactions to continue.

Exercise Independent Judgment

The proposed Guidelines provided that in carrying out his or her duty to provide active oversight of bank management, a director should exercise sound, independent judgment. We received no comments on this paragraph and adopt it in the final Guidelines substantially as proposed. In determining whether a board member is adequately objective and independent, the OCC will consider the degree to which the member’s other responsibilities conflict with his or her ability to act in the covered bank’s interest.

Include Independent Directors

Paragraph D. of section III of the proposed Guidelines provided that at least two members of a bank’s board of directors should be independent, i.e., they should not be members of the bank’s or the parent company’s management. In the preamble to the proposal, we noted that this would enable the bank’s board to provide effective, independent oversight of bank management and, to the extent the bank’s independent directors are also members of the parent company’s board, the OCC would expect that such directors would consider the safety and soundness of the bank’s decisions made by the parent company that impact the bank’s risk profile. The proposal also provided that this standard would not supersede other applicable regulatory requirements concerning the composition of a Federal savings association’s board and that these associations must continue to comply with such requirements.

We received a number of comments on this paragraph. Some commenters opposed the requirement for two independent directors. These commenters believe that the bank should have the flexibility to decide the structure of their own board based on their individual business requirements as long as the board appropriately controls risk. One commenter suggested that the requirement for two independent directors not apply to banks with boards of seven or fewer directors and, if the bank can demonstrate that it would be an undue hardship to find two independent directors. A few commenters noted that it would be better to require a percentage of independent directors rather than requiring a specific number. Other commenters supported this requirement.

One commenter noted that our independence standard differed from the Board’s standard in their Dodd-Frank Act section 165 rules and suggested that the OCC adopt the Board’s standard of independence to be consistent. The OCC is retaining the requirement for covered banks to have at least two independent board members. However, as suggested by one commenter, we have revised this provision to be consistent with the Board’s independence standard in its Dodd-Frank Act section 165 rules. The final Guidelines provide that at least two members of the board of each covered bank should not be an officer or employee of the parent company or covered bank and has not been an officer or employee of the parent company or covered bank during the previous three years; should not be a member of the immediate family, as defined in the Board’s Regulation Y of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, as defined in the Board’s Regulation O; and should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.

Provide Ongoing Training to Directors

Paragraph E. of section III of the proposed Guidelines provided that in order to ensure that each member of the board of directors has the knowledge, skills, and abilities needed to meet the standards set forth in the Guidelines, the bank should establish and adhere to a formal, ongoing training program for directors. The proposed Guidelines provided that the training program apply only to independent directors and should include training on: (i) Complex products, services, lines of business, and risks that have a significant impact on the bank; (ii) laws, regulations, and supervisory requirements applicable to the bank; and (iii) other topics identified by the board of directors. Some commenters requested that the OCC reconsider this paragraph, and suggested that it may discourage qualified individuals from serving as bank directors. Other commenters recommended that the board of directors should retain discretion in directing the frequency, scope, and selecting the provider of training to independent board members. However, as suggested by one commenter, we have revised this provision to be consistent with the Board’s independence standard in its Dodd-Frank Act section 165 rules. The final Guidelines provide that at least two members of the board of each covered bank should not be an officer or employee of the parent company or covered bank and has not been an officer or employee of the parent company or covered bank during the previous three years; should not be a member of the immediate family, as defined in the Board’s Regulation Y of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, as defined in the Board’s Regulation O; and should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.

---

54 See 12 CFR 163.33.
55 Several commenters also suggested that the OCC coordinate with the Board to ensure that these Guidelines are consistent with the Board’s enhanced prudential standards relating to risk management that were issued under section 165 of the Dodd-Frank Act. See 12 U.S.C. 5365. The Board’s enhanced prudential standards apply to a covered bank’s holding company and commenters raised concerns that inconsistencies could create unnecessary burden. We note that OCC staff met with Board staff to discuss the relationship between these Guidelines and the Board’s section 165 rules. The independence standard for directors in the final Guidelines is an example of the OCC’s efforts to address potential inconsistencies.
56 12 CFR 225.41(b)(3).
57 12 CFR 215.2(e)(1).
board members. These commenters also suggested that the training program should only include training on material laws, regulations, and supervisory requirements, and that the final Guidelines should permit banks to choose training suited to their business model, risk profile, and the background of board members. Another commenter suggested that the OCC revise this paragraph to enable a bank’s independent risk management and/or internal audit units to recommend training to the board of directors.

After considering the comments, the OCC has revised this paragraph in the final Guidelines to apply to all directors but to provide more flexibility to the board of directors in structuring a formal, ongoing training program for directors. Specifically, the final Guidelines incorporate commenters’ suggestions and provide that the training program should consider the directors’ knowledge and experience and the covered bank’s risk profile. This revision reflects the OCC’s belief that the training program should be tailored to the director’s needs, experience, and education. Similarly, the final Guidelines provide more flexibility to covered banks to focus the training program on material topics because the final Guidelines emphasize that the program should include training on “appropriate” areas. The OCC also notes that covered banks retain discretion in directing the program’s frequency, scope, and selecting the provider of training under the final Guidelines.

The OCC continues to believe that the board of directors should be financially knowledgeable and committed to conducting diligent reviews of the covered bank’s management team, financial status, and business plans. OCC examiners will evaluate each director’s knowledge and experience, as demonstrated in their written biography and discussions with examiners.

Self-Assessments

Paragraph F. of section III of the proposed Guidelines provided that the bank’s board of directors should conduct an annual self-assessment that includes an evaluation of the board’s effectiveness in meeting the standards provided in section III of the Guidelines.

The OCC received no comments and is adopting this paragraph as proposed. The OCC notes that the self-assessment discussed in this paragraph can be part of a broader self-assessment process conducted by the board of directors, and should result in a constructive dialogue among board members that identifies opportunities for improvement and leads to specific changes that are capable of being tracked, measured, and evaluated. For example, these may include broad changes that range from changing the board of directors’ composition and structure, meeting frequency and agenda items, board report design or content, ongoing training program design or content, and other process and procedure topics.

Relationship Between the Guidelines and OCC’s Heightened Expectations Program

As discussed above, the final Guidelines will supersede the current heightened expectations program. The informal guidance communicated in a Deputy Comptroller memo and “one page” documents will no longer be used to evaluate covered banks. Examiners will assess covered bank governance and risk management practices using these final Guidelines and other existing OCC policy guidance such as handbooks and bulletins to identify appropriate practices and weaknesses and communicate areas needing improvement to the board of directors and management of covered banks according to existing supervisory processes as described in the “Bank Supervision Processes” booklet of the Comptroller’s Handbook.

Integration of Federal Savings Associations Into Part 30

As noted above, 12 CFR parts 30 and 170 establish safety and soundness rules and guidelines for national banks and Federal savings associations, respectively. The OCC proposed to make part 30 and its respective appendices applicable to both national banks and Federal savings associations. The OCC also proposed to remove part 170, as it would no longer be necessary, and to make other minor changes to part 30, including the deletion of references to rescinded OTS guidance. We received no comments on these amendments and therefore adopt them as proposed, with minor technical drafting corrections. These amendments are described below.

Safety and Soundness Rules. On July 10, 1995, the Federal banking agencies adopted a final rule establishing deadlines for submission and review of safety and soundness compliance plans. The final rule provides that the agencies may require compliance plans to be filed by an insured depository institution for failure to meet the safety and soundness standards prescribed by guideline pursuant to section 39 of the FDIA. The safety and soundness rules for national banks and Federal savings associations are set forth at 12 CFR parts 30 and 170, respectively, and, with one exception discussed below, they are substantively the same.

Twelve CFR part 30 establishes the procedures a national bank must follow if the OCC determines that the bank has failed to satisfy a safety and soundness standard or if the OCC requests the bank to file a compliance plan. Section 30.4(d) provides that if a bank fails to submit an acceptable compliance plan within the time specified by the OCC or fails in any material respect to implement a compliance plan, then the OCC shall require the bank to take certain actions to correct the deficiency. However, if a bank has experienced “extraordinary growth” during the previous 18-month period, then the rule provides that the OCC may be required to take certain action to correct the deficiency. Section 30.4(d)(2) defines “extraordinary growth” as “an increase in assets of more than 7.5 percent during any quarter within the 18-month period preceding the issuance of a request for submission of a compliance plan.”

Twelve CFR part 170 sets forth nearly identical safety and soundness rules for Federal savings associations to those applicable in part 30. However, in contrast to part 30, part 170 does not define “extraordinary growth.” Instead, the OCC determines whether a savings association has undergone extraordinary growth on a case-by-case basis by considering various factors such as the association’s management, asset quality, capital adequacy, interest rate risk profile, and operating controls and procedures.

In order to streamline and consolidate the safety and soundness rules applicable to national banks and Federal savings associations, the OCC is applying part 30 to Federal savings associations. This change will not subject Federal savings associations to any new requirements but will subject them to the section 30.4(d)(2) definition of “extraordinary growth.” This definition incorporates an objective standard for determining “extraordinary growth” that is based on an increase in assets over a period of time and will provide greater clarity and guidance to Federal savings associations on when

---

54 This provision applies to all directors because directors that are members of management may not have expertise in all matters for which the board of directors may be providing oversight.

the OCC would be required to take action to correct a deficiency.

Guidelines Establishing Standards for Safety and Soundness. In conjunction with the final rule establishing deadlines for compliance plans, the agencies jointly adopted Interagency Guidelines Establishing Standards for Safety and Soundness (Safety and Soundness Guidelines) as Appendix A to each of the agencies’ respective safety and soundness rules. The Safety and Soundness Guidelines are set forth in Appendix A to parts 30 and 170 for national banks and savings associations, respectively. The texts of Appendix A for national banks and savings associations are substantively identical. Pursuant to section 39 of the FDIA, by adopting the safety and soundness standards as guidelines, the OCC may pursue the course of action that it determines to be most appropriate, taking into consideration the circumstances of a national bank’s noncompliance with one or more standards, as well as the bank’s self-corrective and remedial responses.

In order to streamline and consolidate all safety and soundness guidelines in one place, this final rule amends Appendix A to part 30 so that it also applies to Federal savings associations. This change will not result in any new requirements for Federal savings associations.

Guidelines Establishing Information Security Standards. Section 501 of the Gramm-Leach-Bliley Act requires the Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission to establish appropriate standards relating to administrative, technical, and physical safeguards for customer records and information for the financial institutions subject to their respective jurisdictions. Section 505(b) requires the agencies to implement these standards in the same manner, to the extent practicable, as the standards prescribed pursuant to section 39(a) of the FDIA. Guidelines implementing the requirements of section 501, Interagency Guidelines Establishing Information Security Standards, are set forth in Appendix B to parts 30 and 170 for national banks and Federal savings associations, respectively.63 The texts of Appendix B for national banks and savings associations are substantively identical.

In order to streamline and consolidate all safety and soundness guidelines in one place, the OCC is amending Appendix B to part 30 so that it also applies to Federal savings associations. This change will not result in any new requirements for Federal savings associations.

Guidelines Establishing Standards for Residential Mortgage Lending Practices. On February 7, 2005, the OCC adopted guidelines establishing standards for residential mortgage lending practices for national banks and their operating subsidiaries as Appendix C to part 30.62 These guidelines address certain residential mortgage lending practices that are contrary to safe and sound banking practices, may be conducive to predatory, abusive, unfair or deceptive lending practices, and may warrant a heightened degree of care by lenders.

While there is no equivalent to Appendix C in part 170, Federal savings associations are subject to guidance on residential mortgage lending.63 For many of the same reasons that the OCC decided to incorporate its residential mortgage lending guidance into a single set of guidelines adopted pursuant to section 39, the OCC is now applying Appendix C to Federal savings associations. As a result, Federal savings associations will be subject to the same guidance on residential mortgage lending as national banks, thereby harmonizing residential mortgage lending standards for both types of institutions. Moreover, the application of Appendix C to Federal savings associations clarifies the residential mortgage lending standards applicable to these institutions and enhances the overall safety and soundness of Federal savings associations, because the Appendix C guidelines are enforceable pursuant to the FDIA section 39 process as implemented by part 30. It should be noted, however, that although the guidelines in Appendix C incorporate and implement some of the principles set forth in current Federal savings association guidance on residential real estate lending, they do not replace such guidance.

62 See 70 FR 6329. Appendix C currently applies to national banks, Federal branches and agencies of foreign banks, and any operating subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).


Description of Technical Amendments to Part 30

We also are including in this final rule technical and conforming amendments to the part 30 regulations to add references to new Appendix D, which contains the Guidelines, where appropriate.

The Guidelines are enforceable, pursuant to section 39 of the FDIA and part 30, as we have described. That enforcement mechanism is not necessarily exclusive, however. Nothing in the Guidelines in any way limits the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law. Thus, for example, a bank’s failure to comply with the standards set forth in these Guidelines may also be actionable under section 8 of the FDIA if the failure constitutes an unsafe or unsound practice.

In addition, we are replacing the cross-references to 12 CFR 40.3, the OCC’s former privacy rule, with the appropriate cite to the Consumer Financial Protection Bureau’s (CFPB) privacy rule, 12 CFR 1016.3, in the definition of “customer” and “customer information” in Appendix B to part 30. The Dodd-Frank Act transferred to the CFPB Federal rulemaking authority to issue privacy rules applicable to national banks, as well as Federal savings associations. As a result, 12 CFR part 40 is no longer operative and national banks now must comply with these rules as reissued by the CFPB.64 Lastly, in 12 CFR 168.5, we have replaced the reference to part 170 with part 30 to reflect the fact that this final rule removes part 170 and applies part 30 and its appendices to Federal savings associations.

Regulatory Analysis

Paperwork Reduction Act

The OCC has determined that the final Guidelines involve information collection requirements pursuant to the provisions of the Paperwork Reduction Act of 1995 (the PRA) (44 U.S.C. 3501 et seq.). The OCC may not conduct or sponsor, and an organization is not required to respond to, these information collection requirements unless the information collection displays a currently valid Office of Management and Budget (OMB) control number. The OCC has submitted this collection to OMB pursuant to section 3507(d) of the PRA.

64 The OCC removed 12 CFR part 40 from the Code of Federal Regulations earlier this year. 79 FR 15639 (Mar. 21, 2014).
and section 1320.11 of OMB’s implementing regulations (5 CFR part 1320).

The OCC submitted this collection to OMB at the proposed rule stage as well. OMB filed comments instructing the OCC to examine public comment in response to the proposed rule and describe in the supporting statement of its next collection any public comments received regarding the collection as well as why (or why it did not) incorporate the commenter’s recommendation. The OCC received no comments regarding the collection.

Abstract

The information collection requirements are found in 12 CFR part 30, Appendix D, which establishes minimum standards for the design and implementation of a risk governance framework for insured national banks, insured Federal savings associations, and insured Federal branches of a foreign bank with average total consolidated assets equal to or greater than $50 billion. Insured national banks and insured Federal savings associations with average total consolidated assets of less than $50 billion will also be subject to the Guidelines if that institution’s parent company controls at least one insured national bank or insured Federal savings association with average total consolidated assets equal to or greater than $50 billion. The OCC reserves the authority to apply these requirements to an insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank that has average total consolidated assets of less than $50 billion if the OCC determines that its operations are highly complex or otherwise present a heightened risk.

Standards for Risk Governance Framework

Covered banks should establish and adhere to a formal, written risk governance framework designed by independent risk management. It should include delegations of authority from the board of directors to management committees and executive officers as well as risk limits established for material activities. It should be approved by the board of directors or the board’s risk committee and reviewed and updated at least annually by independent risk management.

Front Line Units

Front line units should take responsibility and be held accountable by the CEO and the board of directors for appropriately assessing and effectively managing all of the risks associated with their activities. In fulfilling this responsibility, each front line unit should, either alone or in conjunction with another organizational unit that has the purpose of assisting a front line unit: (i) Assess, on an ongoing basis, the material risks associated with its activities and use such risk assessments as the basis for fulfilling its responsibilities and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the unit’s risk profile or other conditions; (ii) establish and adhere to a set of written policies that include front line unit risk limits. Such policies should ensure risks associated with the front line unit’s activities are effectively identified, measured, monitored, and controlled, consistent with the covered bank’s risk appetite statement, concentration risk limits, and all policies established within the risk governance framework; (iii) establish and adhere to procedures and processes, as necessary to maintain compliance with the policies described in (ii); (iv) adhere to all applicable policies, procedures, and processes established by independent risk management; (v) develop, attract, and retain talent and maintain staffing levels required to carry out the unit’s role and responsibilities effectively; (vi) establish and adhere to talent management processes; and (vii) establish and adhere to compensation and performance management programs.

Independent Risk Management

Independent risk management should oversee the covered bank’s risk-taking activities and assess risks and issues independent of the front line units by: (i) Designing a comprehensive written risk governance framework commensurate with the size, complexity, and risk profile of the covered bank; (ii) identifying and assessing, on an ongoing basis, the covered bank’s material aggregate risks; (iii) establishing and adhering to enterprise policies that include concentration risk limits; (iv) establishing and adhering to procedures and processes, to ensure compliance with policies in (iii); (v) identifying and communicating to the CEO and board of directors or board’s risk committee material risks and significant instances where independent risk management’s assessment of risk differs from the CEO, and significant instances where the CEO is not adhering to, or holding front line units accountable for adhering to, the risk governance framework; and (vii) developing, attracting, and retaining talent and maintaining staffing levels required to carry out the unit’s role and responsibilities effectively while establishing and adhering to talent management processes and compensation and performance management programs.

Internal Audit

Internal audit should ensure that the covered bank’s risk management framework complies with the Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank. It should maintain a complete and current inventory of all of 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. It should establish and adhere to an audit plan, which is periodically reviewed and updated, that takes into account the covered bank’s risk profile, emerging risks, issues, and establishes the frequency with which activities should be audited. The audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by front line units and independent risk management under the risk governance framework. Significant changes to the audit plan should be communicated to the board’s audit committee. Internal audit should report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan to the board’s audit committee. Reports should identify the root cause of any material issue and include: (i) A determination of whether the root cause creates an issue that has an impact on one organizational unit or multiple organizational units within the covered bank; and (ii) a determination of the effectiveness of front line units and independent risk management in identifying and resolving issues in a timely manner. Internal audit should establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis. The independent assessment should include a conclusion on the covered bank’s compliance with the standards set forth in the Guidelines. Internal audit should
identify and communicate to the board of directors or board’s audit committee significant instances where front line units or independent risk management are not adhering to the risk governance framework. Internal audit should establish a quality assurance program that ensures internal audit’s policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed. Internal audit should develop, attract, and retain talent and maintain staffing levels required to effectively carry out its role and responsibilities. Internal audit should establish and adhere to a comprehensive written statement outlining its role and responsibilities. Internal audit should develop, attract, and retain talent and maintain staffing levels required to effectively carry out its role and responsibilities.

Risk Limit Breaches

A covered bank should establish and adhere to processes that require front line units and independent risk management to: (i) Identify breaches of the risk appetite statement, concentration risk limits, and front line unit risk limits; (ii) distinguish breaches based on the severity of their impact; (iii) establish protocols for disseminating information regarding a breach; (iv) provide a written description of the breach resolution; and (v) establish accountability for reporting and resolving breaches.

Concentration Risk Management

The risk management framework should include policies and supporting processes appropriate for the covered bank’s size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the covered bank’s concentrations of risk.

Risk Data Aggregation and Reporting

This 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 covered bank’s size, complexity, and risk profile and support supervisory reporting requirements. Collectively, these policies, procedures, and processes should provide for: (i) The design, implementation, and maintenance of a data architecture and information technology infrastructure that supports the covered bank’s risk aggregation and reporting needs during normal times and during times of stress; (ii) the capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC; and (iii) the distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

Talent Management and Compensation

A covered bank should establish and adhere to processes for talent development, recruitment, and succession planning. The board of directors or appropriate committee should review and approve a written talent management program. A covered bank should also establish and adhere to compensation and performance management programs that comply with any applicable statute or regulation.

Board of Directors Training and Evaluation

The board of directors of a covered bank should establish and adhere to a formal, ongoing training program for all directors. The board of directors should also conduct an annual self-assessment.

Additionally, commenters should send a copy of their comments to the OMB desk officer for the agencies by mail to the Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, New Executive Office Building, Room 10235, 725 17th Street NW., Washington, DC 20503; by fax to (202) 395–6974; or by email to oira.submission@omb.eop.gov.

Regulatory Flexibility Analysis

The Regulatory Flexibility Act (RFA), 5 U.S.C. 601 et seq., requires generally that, in connection with a rulemaking, an agency prepare and make available for public comment a regulatory flexibility analysis that describes the impact of a rule on small entities. However, the regulatory flexibility analysis otherwise required under the RFA is not required if an agency certifies that the rule will not have a significant economic impact on a substantial number of small entities (defined in regulations promulgated by the Small Business Administration (SBA) to include banking organizations with total assets of less than or equal to $550 million) and publishes its certification and a brief explanatory statement in the Federal Register together with the rule.

As of December 31, 2013, the OCC supervised 1,231 small entities based on the SBA’s definition of small entities for RFA purposes. As discussed in the SUPPLEMENTARY INFORMATION above, the final Guidelines will generally be applicable only to OCC-supervised institutions that have average total consolidated assets of $50 billion or greater; therefore no small entities will be affected by the final Guidelines. Although the application of part 30 to Federal savings associations will affect a substantial number of small Federal savings associations, we do not associate any cost to this change. As such, pursuant to section 605(b) of the RFA, the OCC certifies that these final rules and guidelines will not have a significant economic impact on a substantial number of small entities.

Unfunded Mandates Reform Act Analysis

The OCC has analyzed the final rules and guidelines under the factors in the Unfunded Mandates Reform Act of 1995 (UMRA) (2 U.S.C. 1532). Under this analysis, the OCC considered whether the final rules and guidelines will result in expenditures by State, local, and tribal governments, or the private sector, of $100 million or more in any one year (adjusted annually for inflation). The OCC has determined that the final rules and guidelines will not result in expenditures by State, local, and tribal governments, or the private sector, of $100 million or more in any one year. Accordingly, the final rules and guidelines are not subject to section 202 of the UMRA.

List of Subjects

12 CFR Part 30

Banks, Banking, Consumer protection, National banks, Privacy, Safety and soundness, Reporting and recordkeeping requirements.

12 CFR Part 168

Consumer protection, Privacy, Reporting and recordkeeping requirements, Savings associations, Security measures.

12 CFR Part 170

Accounting, Administrative practice and procedure, Bank deposit insurance, Reporting and recordkeeping requirements, Safety and soundness, Savings associations.

For the reasons set forth in the preamble, and under the authority of 12 U.S.C. 93a, chapter 1 of title 12 of the Code of Federal Regulations is amended as follows:

PART 30—SAFETY AND SOUNDNESS STANDARDS

1. The authority citation for part 30 is revised to read as follows:

Authority: 12 U.S.C. 1, 93a, 371, 1462a, 1463, 1464, 1467a, 1818, 1826, 1831p–1, 1861–1864, 3102(b) and 5412(b)(2)(B); 15 U.S.C. 1681s, 1681w, 6801, and 6805(b)(1).

§ 30.1 [Amended]

■ 2. Section 30.1 is amended by:

a. In paragraph (a):
   ■ i. Removing “appendices A, B, and C” and adding in its place “appendices A, B, C, and D”;
   ■ ii. Removing the phrase “and federal branches of foreign banks.” and adding in its place the phrase “Federal savings associations, and Federal branches of foreign banks”;

b. In paragraph (b):
   ■ i. Removing the word “federal” wherever it appears and adding “Federal” in its place;
   ■ ii. Adding the phrase “Federal savings associations, and” after the phrase “national bank.”;
   ■ iii. Removing the phrase “branch or” and adding in its place the word “branch and”;
   ■ iv. Adding a comma after the word “companies”.

■ 3. Section 30.2 is amended by:

■ a. Removing in the second and third sentence the word “bank” and adding in its place the phrase “national bank or Federal savings association”; and

■ b. Adding a final sentence to read as follows:

§ 30.2 Purpose.

* * * The OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches are set forth in appendix D to this part.

■ 4. Section 30.3 is amended by:

a. Revising the section heading;

b. Removing the phrase “a bank”, wherever it appears, and adding in its place the phrase “a national bank or Federal savings association”;

■ c. In paragraph (a), removing “the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part, or the OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices set forth in appendix C to this part” and adding in its place “the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part, the OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices set forth in appendix C to this part, or the OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches set forth in appendix D to this part”;

d. In paragraph (b), adding the phrase “to satisfy” after the word “failed”; and

e. In paragraph (b), removing the phrase “the bank” and adding in its place the phrase “the bank or savings association”.

The revision reads as follows:

§ 30.3 Determination and notification of failure to meet safety and soundness standards and request for compliance plan.

* * * * *

§ 30.4 [Amended]

■ 5. Section 30.4 is amended by:

a. In paragraphs (a), (d), and (e), removing the phrases “A bank” and “a bank”, wherever they appear, and adding in their place the phrases “A national bank or Federal savings association” and “a national bank or Federal savings association”, respectively;

b. In paragraph (a), the first sentence of paragraph (d)(1), and in paragraph (e), adding after the phrase “the bank”, the phrase “or savings association”;

c. In paragraph (b), removing the word “bank”, and adding in its place the
Part 30; for the Board of Governors of the Federal Reserve System, these regulations appear at 12 CFR part 263; and for the Federal Deposit Insurance Corporation, these regulations appear at 12 CFR part 308, subpart R and 12 CFR part 391, subpart B.

9. Appendix B to part 30 is amended by:

a. Removing the words “bank” and “bank’s”, wherever they appear, except in Sections I.A., I.C.2.a., and I.C.2.d., and adding in their place the phrase “national bank or Federal savings association”;
b. In Section I.A., removing the phrase “bank” wherever it appears, except in the previous 24-month period, or the bank’s”, wherever they appear, except in Sections I.A., I.C.2.a., and I.C.2.d., and adding in their place the phrase “national bank or Federal savings association”;
c. In Section I.C.2.d., removing the phrase “§ 40.3(h) of this chapter” and adding in its place the phrase “12 CFR 1016.3(i)”; and
d. In Section I.C.2.e., removing the phrase “§ 40.3(n) of this chapter” and adding in its place the phrase “12 CFR 1016.3(p)”; and
e. In Supplement A to Appendix B to part 30, by revising footnotes 1, 2, 9, 11, and 12.

The revisions read as follows:

Appendix B to Part 30—Interagency Guidelines Establishing Information Security Standards

* * * * *

Supplement A to Appendix B to Part 30—Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

* * * * *

1 This Guidance was jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). Pursuant to 12 U.S.C. 5412, the OTS is no longer a party to this Guidance.


9 Under the Guidelines, an institution’s customer information systems consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. See Security Guidelines, I.C.2.d.

* * * * *


12 An institution’s obligation to file a SAR is set out in the Agencies’ SAR regulations and Agency guidance. See 12 CFR 21.11 (national banks, Federal branches and agencies); 12 CFR 163.180 (Federal savings associations); 12 CFR 208.62 (State member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured State branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (State non-member banks); and 12 CFR 390.355 (state savings associations). National banks and Federal savings associations must file SARs in connection with computer intrusions and other computer crimes. See OCC Bulletin 2000–14, “Infrastructure Threats—Intrusion Risks” (May 15, 2000); see also Federal Reserve SR 01–11, Identity Theft and Pretexet Calling, Apr. 26, 2001.

* * * * *

10. Appendix C to part 30 is amended by:

a. In sections I.v., II.B.1., II.B.2., III.A. introductory text, III.B. introductory text, III.B.6., III.C., III.E.4., and III.E.6., removing the word “bank” wherever it appears, and adding in its place the phrase “national bank or Federal savings association”;
b. In section II.B. introductory text and III.D., removing the word “bank’s” and adding in its place the phrase “national bank’s or Federal savings association’s”;
c. In sections II.B.1. and III.B.6., removing the word “bank’s” and adding in its place the phrase “bank’s or savings association’s”; and
d. Revising the second sentence of section I.i., first two sentences of section I.ii., section I.v.i., sections I.A., I.C., I.D.2.b., II.A., III.E. introductory text, III.E.5., and III.F.

The revisions read as follows:

Appendix C to Part 30—OCC Guidelines Establishing Standards for Residential Mortgage Lending Practices

* * * * *

I. * * * * 

1. * * * * The Guidelines are designed to protect against involvement by national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and their respective operating subsidiaries (together, “national banks and Federal savings associations”), either directly or through loans that they purchase or make through intermediaries, in predatory or abusive residential mortgage lending
practices that are injurious to their respective customers and that expose the national bank or Federal savings association to credit, legal, compliance, reputation, and other risks.

iii. In addition, national banks, Federal savings associations, and their respective operating subsidiaries must comply with the requirements and Guidelines affecting appraisals of residential mortgage loans and appraiser independence. 12 CFR part 34, subpart C, and the Interagency Appraisal and Evaluation Guidelines (OCC Bulletin 2010–42 (December 10, 2010)).

vi. Finally, OCC regulations and supervisory guidance on fiduciary activities and asset management address the need for national banks and Federal savings associations to perform due diligence and exercise appropriate control with regard to trustee activities. See 12 CFR 9.6 (a), in the case of national banks, and 12 CFR 150.200, in the case of Federal savings associations, and the Comptroller’s Handbook on Asset Management. For example, national banks and Federal savings associations should exercise appropriate diligence to minimize potential reputation risks when they undertake to act as trustees in mortgage securitizations.

A. Scope. These Guidelines apply to the residential mortgage lending activities of national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and operating subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

C. Relationship to Other Legal Requirements. Actions by a national bank or Federal savings association in connection with residential mortgage lending that are inconsistent with these Guidelines or Appendix A to this part 30 may also constitute unsafe or unsound practices for purposes of section 6 of the Federal Deposit Insurance Act, 12 U.S.C. 1818, unfair or deceptive practices for purposes of section 5 of the FTC Act, 15 U.S.C. 45, and the OCC’s Lending Rules, 12 CFR 34.3 (Lending Rules) and Real Estate Lending Standards, 12 CFR part 34, subpart D, in the case of national banks, and 12 CFR 160.100 and 160.101, in the case of Federal savings associations, or violations of the ECOA and FHA.

b. National bank or Federal savings association means any national bank, Federal savings association, Federal branch or Federal agency of a foreign bank, and any operating subsidiary thereof that is subject to these Guidelines.

11. A new Appendix D is added to part 30 to read as follows:

Appendix D to Part 30—OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches

Table of Contents

I. Introduction

A. Scope

B. Compliance Date

C. Reservation of Authority

D. Preservation of Existing Authority

E. Definitions

II. Standards For Risk Governance Framework

A. Risk Governance Framework

B. Scope of Risk Governance Framework

C. Roles and Responsibilities

1. Role and Responsibilities of Front Line Units

2. Role and Responsibilities of Independent Risk Management

3. Role and Responsibilities of Internal Audit

D. Strategic Plan

E. Risk Appetite Statement

F. Concentration and Front Line Unit Risk Limits

G. Risk Appetite Review, Monitoring, and Communication Processes

H. Processes Governing Risk Limit Breaches

I. Concentration Risk Management

J. Risk Data Aggregation and Reporting

K. Relationship of Risk Appetite Statement, Concentration Risk Limits, and Front Line Unit Risk Limits to Other Processes

L. Talent Management Processes

M. Compensation and Performance Management Programs

III. Standards for Board of Directors

A. Require an Effective Risk Governance Framework

B. Provide Active Oversight of Management

C. Exercise Independent Judgment

D. Include Independent Directors

E. Provide Ongoing Training to All Directors

F. Self-Assessments

I. Introduction

1. The OCC expects a covered bank, as that term is defined in paragraph I.E. to establish and implement a risk governance framework to manage and control the covered bank’s risk-taking activities.

2. This appendix establishes minimum standards for the design and implementation of a covered bank’s risk governance framework and minimum standards for the covered bank’s board of directors in providing oversight to the framework’s design and implementation (Guidelines). These standards are in addition to any other applicable requirements in law or regulation.

3. A covered bank may use its parent company’s risk governance framework in its entirety, without modification, if the framework meets these minimum standards, the risk profiles of the parent company and the covered bank are substantially the same as set forth in paragraph I.A. of these Guidelines, and the covered bank has demonstrated through a documented assessment that its risk profile and its parent company’s risk profile are substantially the same. The assessment should be conducted at least annually, in conjunction with the review and update of the risk governance framework performed by independent risk management, as set forth in paragraph II.A. of these Guidelines.

4. A parent company’s and covered bank’s risk profiles are substantially the same if, as reported on the covered bank’s Federal Financial Institutions Examination Council Consolidated Reports of Condition and Income (Call Reports) for the four most recent consecutive quarters, the covered bank’s average total consolidated assets, as
calculated according to paragraph I.A. of these Guidelines, represent 95 percent or more of the parent company’s average total consolidated assets. A covered bank that does not satisfy this test may submit a written analysis to the OCC for consideration and approval that these Guidelines are not the risk profile of the covered bank and the covered bank are substantially the same based upon other factors not specified in this paragraph.

5. Subject to paragraph 1.B. of these Guidelines, a covered bank should establish its own risk governance framework when the parent company’s and covered bank’s risk profiles are not substantially the same. The covered bank’s framework should ensure that the covered bank’s risk profile is easily distinguished and separate from that of its parent for risk management and supervisory reporting purposes and that the safety and soundness of the covered bank is not jeopardized by decisions made by the parent bank’s company’s board of directors and management.

6. When the parent company’s and covered bank’s risk profiles are not substantially the same, a covered bank may, in consultation with the OCC, incorporate or rely on components of its parent company’s risk governance framework when developing its own risk governance framework to the extent those components are consistent with the objectives of these Guidelines.

A. Scope

These Guidelines apply to any bank, as that term is defined in paragraph I.E. of these Guidelines, with average total consolidated assets equal to or greater than $50 billion. In addition, these Guidelines apply to any bank with average total consolidated assets less than $50 billion if that institution’s parent company controls at least one covered bank. For a covered bank, average total consolidated assets means the average of the covered bank’s total consolidated assets, as reported on the covered bank’s Call Reports, for the four most recent calendar quarters.

B. Compliance Date

1. Initial compliance. The date on which a covered bank should comply with the Guidelines is set forth below:

(a) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, equal to or greater than $750 billion as of November 10, 2014 should comply with these Guidelines on the date that such other covered bank should comply; and
(b) A covered bank with average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, less than $50 billion, if that institution’s parent company controls at least one other covered bank as of November 10, 2014 should comply with these Guidelines on the date that such other covered bank should comply; and
(c) A covered bank that does not come within the scope of these Guidelines on November 10, 2014, but subsequently becomes subject to the Guidelines because average total consolidated assets, as calculated according to paragraph I.A. of these Guidelines, are equal to or greater than $50 billion after November 10, 2014, should comply with these Guidelines within 18 months from the as-of date of the most recent Call Report used in the calculation of the average.

C. Reservation of Authority

1. The OCC reserves the authority to apply these Guidelines in whole or in part, to a bank that has average total consolidated assets less than $50 billion, if the OCC determines such bank’s operations are highly complex or otherwise present a heightened risk as to warrant the application of these Guidelines.

2. The OCC reserves the authority, for each covered bank, to extend the time for compliance with these Guidelines or modify these Guidelines; or

3. The OCC reserves the authority to determine that compliance with these Guidelines should no longer be required for a covered bank. The OCC would generally make the determination under this paragraph I.C.3 if a covered bank’s operations are no longer highly complex or no longer present a heightened risk. In determining whether a covered bank’s operations are highly complex or present a heightened risk, the OCC will consider the following factors:

   Complexity of products and services, risk profile, and scope of operations.

4. When exercising the authority in this paragraph I.C., the OCC will apply notice and response procedures, when appropriate, in the same manner and to the same extent as the notice and response procedures in 12 CFR 3.404.

D. Preservation of Existing Authority

Neither section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p–1) nor these Guidelines in any way limit the authority of the OCC to address unsafe or unsound practices or conditions or other violations of law. The OCC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to any other enforcement action available to the OCC.

E. Definitions

1. Bank means any insured national bank, insured Federal savings association, or insured Federal branch of a foreign bank.

2. Chief Audit Executive means an individual who leads internal audit and is

3. Covered bank means any bank:

   (a) Owns, controls, or holds with power to vote 25 percent or more of the voting securities of the covered bank; or

   (b) Consolidates the covered bank for financial reporting purposes.

4. Covered bank means any bank:

   (a) Owns, controls, or holds with power to vote 25 percent or more of the class of voting securities of the covered bank; or

   (b) Consolidates the covered bank for financial reporting purposes.

5. Covered bank means any bank:

   (a) Owns, controls, or holds with power to vote 25 percent or more of the class of voting securities of the covered bank; or

   (b) Consolidates the covered bank for financial reporting purposes.

6. Front Line Unit. (a) Except as provided in paragraph (b) of this definition, front line unit means any organizational unit or function thereof in a covered bank that is accountable for a risk in a covered bank.

7. Independent risk management means any organizational unit within a covered bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Such units maintain independence from front line units through the following reporting structure:

   (a) The board of directors or the board’s risk committee reviews and approves the risk governance framework.

   (b) Each Chief Risk Executive has unrestricted access to the board of directors and its committees to address risks and issues identified through independent risk management’s activities.

   (c) The board of directors or its risk committee approves all decisions regarding the appointment or removal of the Chief Risk Executive(s) and approves the annual compensation and salary adjustment of the Chief Risk Executive(s); and

   (d) No front line unit executive oversees any independent risk management unit.

8. Internal audit means the organizational unit within a covered bank that is designated one level below the Chief Executive Officer in a covered bank’s organizational structure.
to fulfill the role and responsibilities outlined in 12 CFR part 30, Appendix A, II.B. Internal audit maintains independence from front line units and independent risk management through the following reporting structure:

(a) The Chief Audit Executive has unrestricted access to the board’s audit committee to address risks and issues identified through internal audit’s activities;
(b) The audit committee reviews and approves internal audit’s overall charter and audit plan;
(c) The audit committee approves all decisions regarding the appointment or removal and annual compensation and salary adjustment of the Chief Audit Executive;
(d) The audit committee or the Chief Audit Executive oversees the Chief Audit Executive’s administrative activities; and
(e) No front line unit executive oversees internal audit.

9. Parent company means the top-tier legal entity in a covered bank’s ownership structure.

10. Risk appetite means the aggregate level and types of risk the board of directors and management are willing to assume to achieve a covered bank’s strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements.

11. Risk profile means a point-in-time assessment of a covered bank’s risks, aggregated within and across each relevant risk category, using methodologies consistent with the risk appetite statement described in paragraph II.E. of these Guidelines.

II. Standards for Risk Governance Framework

A. Risk governance framework. A covered bank should establish and adhere to a formal, written risk governance framework that is designed by independent risk management and approved by the board of directors or the board’s risk committee. The risk governance framework should include delegations of authority from the board of directors to management committees and executive officers as well as the risk limits established for material activities. Independent risk management 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.

B. Scope of risk governance framework. The risk governance framework should cover the following risk categories that apply to the covered bank:

- Credit risk
- Interest rate risk
- Liquidity risk
- Price risk
- Operational risk
- Compliance risk
- Strategic risk
- Reputation risk.

C. Roles and responsibilities. The risk governance framework should include well-defined risk management roles and responsibilities for front line units, independent risk management, and internal audit.

The roles and responsibilities of each of these organizational units should be:

2 These roles and responsibilities are in addition to any roles and responsibilities set forth in

1. Role and responsibilities of front line units. Front line units should take responsibility and be held accountable by the Chief Executive Officer and the board of directors for appropriately assessing and effectively managing all of the risks associated with their businesses.

(a) In fulfilling this responsibility, each front line unit should, either alone or in conjunction with another organizational unit that has the purpose of assisting a front line unit:

- Assess, on an ongoing basis, the material risks associated with its activities and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs II.C.1.(b) and (c) of these Guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the unit’s risk profile or other conditions;
- Establish and adhere to a set of written policies that include front line unit risk limits as discussed in paragraph II.F. of these Guidelines; and
- Establish and adhere to a set of written plans to address risks associated with the front line unit’s activities, as necessary, to maintain compliance with the policies described in paragraph II.C.1.(b) of these Guidelines;
- Monitor, and control, consistent with the covered bank’s risk appetite statement, concentration risk limits, and all policies established within the risk governance framework under paragraphs II.C.2.(c) and II.G. through K. of these Guidelines;
- Establish and adhere to procedures and processes, as necessary, to maintain compliance with the policies described in paragraph II.C.1.(b) of these Guidelines;
- Develop, attract, and retain talent and maintain staffing levels required to carry out the unit’s role and responsibilities effectively, as set forth in paragraphs II.C.1.(a) through (d) of these Guidelines;
- Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and
- Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

2. Role and responsibilities of independent risk management. Independent risk management should oversee the covered bank’s risk-taking activities and assess risks and issues independent of front line units. In fulfilling these responsibilities, independent risk management should:

(a) Take primary responsibility and be held accountable by the Chief Executive Officer and the board of directors or the board’s risk committee:

- Maintain a complete and current inventory of all of 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 framework that meets these Guidelines and is commensurate with the size, complexity, and risk profile of the covered bank;
- Identify and assess, on an ongoing basis, the covered bank’s material aggregate risks and use such risk assessments as the basis for fulfilling its responsibilities under paragraphs II.C.2.(c) and (d) of these Guidelines and for determining if actions need to be taken to strengthen risk management or reduce risk given changes in the covered bank’s risk profile or other conditions;
- Establish and adhere to a set of written policies that include concentration risk limits. Such policies should state how aggregate risks within the covered bank are effectively identified, measured, monitored, and controlled, consistent with the covered bank’s risk appetite statement and all policies and processes established within the risk governance framework under paragraphs II.G. through K. of these Guidelines;
- Establish and adhere to procedures and processes, as necessary, to ensure compliance with the policies described in paragraph II.C.2.(c) of these Guidelines;
- Identify and communicate to the board of directors or the board’s risk committee:

- Significant instances where independent risk management’s assessment of risk differs from that of a front line unit; and
- Significant instances where a front line unit is not adhering to the risk governance framework, including instances when front line units do not meet the standards set forth in paragraph II.C.1. of these Guidelines;
- Identify and communicate to the board of directors or the board’s risk committee:

- Significant instances where independent risk management’s assessment of risk differs from that of the Chief Executive Officer; and
- Significant instances where the Chief Executive Officer is not adhering to, or holding front line units accountable for adhering to, the risk governance framework;
- Develop, attract, and retain talent and maintain staffing levels required to carry out its role and responsibilities effectively, as set forth in paragraphs II.C.2.(a) through (f) of these Guidelines;
- Establish and adhere to talent management processes that comply with paragraph II.L. of these Guidelines; and
- Establish and adhere to compensation and performance management programs that comply with paragraph II.M. of these Guidelines.

3. Role and responsibilities of internal audit. In addition to meeting the standards set forth in appendix A of part 30, internal audit should ensure that the covered bank’s risk governance framework complies with these Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank. In carrying out its responsibilities, internal audit should:

(a) Maintain a complete and current inventory of all of 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

Appendices A, B, and C to Part 30. Many of the risk management practices established and maintained by a covered bank to meet these standards, including loan review and credit underwriting and administration practices, should be components of its risk governance framework, within the construct of the three distinct units identified herein. In addition, existing OCC guidance sets forth standards for establishing risk management programs for certain risks, e.g., compliance risk management. These programs should also be considered components of the risk governance framework, within the context of the three units described in paragraph II.C. of these Guidelines.
described in paragraph II.C.3.(b) of these Guidelines;
(b) Establish and adhere to an audit plan that is periodically reviewed and updated
that takes into account the covered bank’s
risk profile, emerging risks, and issues, and
establishes the frequency with which
activity should be audited. The audit plan
should require internal audit to evaluate the
adequacy of and compliance with policies,
procedures, and processes established by
front line units and independent risk
management under the risk governance
framework. Significant changes to the audit
plan should be communicated to the board’s
audit committee;
(c) Report in writing, conclusions and
material issues and recommendations from
audit work carried out under the audit plan
described in paragraph II.C.3.(b) of these
Guidelines to the board’s audit committee.
Internal audit’s reports to the audit
committee should also identify the root cause
of any material issues and include:
(i) A determination of whether the root
cause was an issue that has an impact on
one organizational unit or multiple
organizational units within the covered bank;
and
(ii) A determination of the effectiveness of
front line units and independent risk
management in identifying and resolving
issues in a timely manner;
(d) Establish and adhere to processes for
independently assessing the design and
ongoing effectiveness of the risk governance
framework on at least an annual basis. The
independent assessment should include a
conclusion on the covered bank’s compliance
with the standards set forth in these
Guidelines;\(^3\)
(e) Identify and communicate to the
board’s audit committee significant instances
where front line units or independent risk
management processes fail to conform
to the risk governance framework;
(f) Establish a quality assurance program
that ensures internal audit’s policies,
procedures, and processes comply with
applicable regulatory and industry guidance,
are appropriate for the size, complexity, and
risk profile of the covered bank, are updated
to reflect changes to internal and external
risk factors, emerging risks, and
improvements in industry internal audit
practices, and are consistently followed;
(g) Develop, attract, and retain talent and
maintain staffing levels required to
effectively carry out its role and
responsibilities, as set forth in paragraphs
II.C.3.(a) through (f) of these Guidelines;
(h) Establish and adhere to talent
management processes that comply with
paragraph II.L. of these Guidelines; and
(i) Establish and adhere to compensation
and performance management programs that
comply with paragraph II.M. of these
Guidelines.

D. Strategic plan. The Chief Executive
Officer should be responsible for the
development of a written strategic plan with

\(^3\)The annual independent assessment of the risk
governance framework may be conducted by
internal audit, an external party, or internal audit
in conjunction with an external party.

input from front line units, independent risk
management, and internal audit. The board
of directors should evaluate and approve the
strategic plan and monitor management’s
efforts to implement the strategic plan at least
annually. The strategic plan should cover, at
a minimum, a three-year period and:
1. Contain a comprehensive assessment of
risks that currently have an impact on the
covered bank or that could have an impact
on the covered bank during the period
covered by the strategic plan;
2. Articulate an overall mission statement
and strategy that is consistent with the
covered bank, and include an explanation of how the
covered bank will achieve those objectives;
3. Include an explanation of how the
covered bank will update, as necessary, the
risk governance framework to account for
changes in the covered bank’s risk profile
projected under the strategic plan; and
4. Be reviewed, updated, and approved, as
necessary, due to changes in the covered
bank’s risk profile or operating environment
that were not contemplated when the
strategic plan was developed.

E. Risk appetite statement. A covered bank
should have a comprehensive written
statement that articulates the covered bank’s
risk appetite and serves as the basis for the
risk governance framework. 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
covered bank will assess and accept risks,
including those that are difficult to quantify.
Quantitative limits should incorporate sound
stress testing processes, as appropriate, and
address the covered bank’s earnings, capital,
and liquidity. The covered bank should set
limits at levels that take into account
appropriate capital and liquidity buffers and
prompt management and the board of
directors to take action before the covered
bank’s risk profile jeopardizes the adequacy
of its earnings, liquidity, and capital.\(^4\)

F. Concentration and front line unit risk
limits. The risk governance framework
should include concentration risk limits and,
as applicable, front line unit risk limits, for
the relevant risks. Concentration and front
line unit risk limits should limit excessive
risk taking and, when aggregated across such
units, provide that these risks do not exceed
the limits established in the covered bank’s
risk appetite statement.

G. Risk appetite review, monitoring, and
communication processes. The risk
governance framework should require:

1. Review and approval of the risk appetite
statement by the board of directors or the
board’s risk committee at least annually or
more frequently, as necessary, 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;
2. Initial communication and ongoing
reinforcement of the covered bank’s risk
appetite statement throughout the covered
bank in a manner that causes all employees
to align their risk-taking decisions with
applicable aspects of the risk appetite
statement;
3. Monitoring by independent risk
management of the covered bank’s risk
profile relative to its risk appetite and
compliance with concentration risk limits
and reporting on such monitoring to the
board of directors or the board’s risk
committee at least quarterly;
4. Monitoring by front line units of
compliance with their respective risk limits
and reporting to independent risk
management at least quarterly; and
5. When necessary due to the level and
type of risk, monitoring by independent risk
management of front line units’ compliance
with front line unit risk limits, ongoing
communication with front line units
regarding adherence to these limits, and
reporting of any concerns to the Chief
Executive Officer and the board of directors
or the board’s risk committee, as set forth in
paragraphs II.C.2.(e) and (f) of these
Guidelines, all at least quarterly.

H. Processes governing risk limit breaches.
A covered bank should establish and adhere
to processes that require front line units and
independent risk management, in
conjunction with their respective
responsibilities, to:
1. Identify breaches of the risk appetite
statement, concentration risk limits, and
front line unit risk limits;
2. Distinguish breaches based on the
severity of their impact on the covered bank;
3. Establish protocols for when and how to
inform the board of directors, front line unit
management, independent risk management,
internal audit, and the OCC of a risk limit
breach that takes into account the severity of
the breach and its impact on the covered
bank;
4. Include in the protocols established in
paragraph II.H.3. of these Guidelines the
requirement to provide a written description
of how a breach will be, or has been,
resolved; and
5. Establish accountability for reporting
and resolving breaches that include
consequences for risk limit breaches that take
into account the magnitude, frequency, and
recurrence of breaches.

I. Concentration risk management. The risk
governance framework should include
policies and supporting processes
appropriate for the covered bank’s size,
complexity, and risk profile for effectively
identifying, measuring, monitoring, and
controlling the covered bank’s concentrations
of risk.

J. Risk data aggregation and reporting. 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:

1. The design, implementation, and maintenance of a data architecture and information technology infrastructure that support the covered bank’s risk aggregation and reporting needs during normal times and during times of stress;

2. The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC; and

3. The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

K. Relationship of risk appetite statement, concentration risk limits, and front line unit risk limits to other processes. A covered bank’s front line units and independent risk management should incorporate at a minimum the risk appetite statement, concentration risk limits, and front line unit risk limits into the following:

1. Strategic and annual operating plans;

2. Capital stress testing and planning processes;

3. Liquidity stress testing and planning processes;

4. Product and service risk management processes, including those for approving new and modified products and services;

5. Decisions regarding acquisitions and divestitures; and

6. Compensation and performance management programs.

1. Talent management processes. A covered bank should establish and adhere to processes for talent development, recruitment, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. The board of directors or an appropriate committee of the Board that apply to Federal savings associations. These institutions must continue to comply with such other requirements.

M. Compensation and performance management programs. A covered bank should establish and adhere to compensation and performance management programs that comply with any applicable statute or regulation and are appropriate to:

1. Ensure the Chief Executive Officer, front line units, independent risk management, and internal audit implement and adhere to an effective risk governance framework;

2. Ensure front line unit compensation plans and decisions appropriately consider the level and severity of issues and concerns identified by independent risk management and internal audit, as well as the timeliness of corrective action to resolve such issues and concerns;

3. Attract and retain the talent needed to design, implement, and maintain an effective risk governance framework; and

4. Prohibit any incentive-based payment arrangement, or any feature of any such arrangement, that encourages inappropriate risks by providing excessive compensation or that could lead to material financial loss.

III. Standards for Board of Directors

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

B. Provide active oversight of management. A covered bank’s board of directors 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 of directors may rely on risk assessments and reports prepared by independent risk management 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.

C. Exercise independent judgment. When providing active oversight under paragraph III.B. of these Guidelines, each member of the board of directors should exercise sound, independent judgment.

D. Include independent directors. To promote effective, independent oversight of the covered bank’s management, at least two members of the board of directors:6

6This provision does not supersede other regulatory requirements regarding the composition of the Board that apply to Federal savings

1. Should not be an officer or employee of the parent company or covered bank and has not been an officer or employee of the parent company or covered bank during the previous three years;

2. Should not be a member of the immediate family, as defined in § 225.41(b)(3) of the Board of Governors of the Federal Reserve System’s Regulation Y (12 CFR 225.41(b)(3)), of a person who is, or has been within the last three years, an executive officer of the parent company or covered bank, as defined in §215.2(e)(1) of Regulation O (12 CFR 215.2(e)(1)); and

3. Should qualify as an independent director under the listing standards of a national securities exchange, as demonstrated to the satisfaction of the OCC.

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

1. Complex products, services, lines of business, and risks that have a significant impact on the covered bank;

2. Laws, regulations, and supervisory requirements applicable to the covered bank; and

3. Other topics identified by the board of directors.

F. Self-assessments. A covered bank's board of directors should conduct an annual self-assessment that includes an evaluation of its effectiveness in meeting the standards in section III of these Guidelines.

PART 168—SECURITY PROCEDURES

12. The authority citation for part 168 continues to read as follows:


§ 168.5 [Amended]

13. Section 168.5 is amended by removing the phrase “part 170” wherever it appears and adding in its place the phrase “part 30”.

PART 170 [REMOVED]


Dated: September 2, 2014.

Thomas J. Curry,
Comptroller of the Currency.

[FR Doc. 2014–21224 Filed 9–10–14; 8:45 am]

BILLING CODE 4810–33–P
To: Deputy Comptrollers, Department and Division Heads, District Counsel, and All Examining Personnel

Purpose and Scope

This *Policies and Procedures Manual* (PPM) issuance revises PPM 5310-3, “Bank Enforcement Actions and Related Matters,” dated October 31, 2017, which establishes general policies and procedures for Office of the Comptroller of the Currency (OCC) staff when the OCC takes enforcement actions against banks in response to violations of laws, regulations, final agency orders, conditions imposed in writing, or written agreements (collectively, violations), or deficient practices, including those that are unsafe or unsound. This PPM provides guidance in selecting the actions best suited to resolve a bank’s deficiencies and promotes consistency while preserving flexibility for individual circumstances.

This PPM applies to the supervision of all banks examined by the OCC. National banks, federal savings associations, and federal branches and agencies are collectively referred to as “banks” in this PPM. When necessary, types of banks are specifically distinguished or excepted.\(^1\)

This PPM does not address enforcement actions against institution-affiliated parties or other individuals, civil money penalty (CMP) actions, or actions to enforce securities laws and regulations.\(^2\) This PPM also does not address conditions imposed in writing or operating agreements issued in the context of a bank’s licensing filing.\(^3\)

This PPM provides internal OCC guidance and does not create substantive or procedural rights enforceable at law or in any administrative proceeding. This PPM also does not supersede or limit the applicability of any other OCC policy that may provide more explicit guidance or

---

\(^1\) The principles in this PPM may be considered in taking an enforcement action against a third-party service provider. Examiners should consult with the appropriate OCC legal staff in the appropriate District Counsel’s office or the Enforcement and Compliance Division on these matters.


\(^3\) For the purposes of this PPM, a “licensing filing” means an application, notice, or other request submitted to the OCC under 12 CFR 5.
establish supplemental procedures applicable to bank enforcement actions or treatment of supervisory or licensing issues arising from the various specialty areas (for example, consumer protection, Bank Secrecy Act (BSA)/anti-money laundering (AML), asset management, or information technology).

Contents

I. Introduction ...................................................................................................................3
II. Types of Bank Enforcement Actions ...........................................................................4
   Informal Bank Enforcement Actions ...........................................................................4
   Formal Bank Enforcement Actions ...........................................................................5

III. Determining the Appropriate Supervisory or Enforcement Response ....................6
   1- and 2-Rated Banks .................................................................................................7
   3-Rated Banks ............................................................................................................7
   4- and 5-Rated Banks .................................................................................................8
   Resolution ..................................................................................................................8

IV. Decision Authority and OCC Legal Staff Responsibilities .........................................8
    Supervision Review Committees .............................................................................8
    OCC Legal Staff Responsibilities .............................................................................9

V. Formal Investigations ..................................................................................................9
VI. Content of Bank Enforcement Actions ......................................................................10
VII. Timeliness of Bank Enforcement Actions ..................................................................11
VIII. Follow-Up Activities ................................................................................................11
IX. Assessing Compliance With Bank Enforcement Actions ........................................12
X. Communicating Bank Enforcement Action Compliance ........................................13
    Bank Submissions and Requests ............................................................................13

XI. Terminating a Bank Enforcement Action ..................................................................14
XII. Documentation in OCC Supervisory Information Systems ....................................15
XIII. Public Disclosure of Bank Enforcement Actions .....................................................16
     Disclosures by Banks .............................................................................................16
Appendix A: Informal Enforcement Actions Against Banks ..............................................18
Appendix B: Formal Enforcement Actions Against Banks ................................................20
Appendix C: Bank Enforcement Action Processes and Time Frames ................................25
Appendix D: Mandatory and Discretionary Provisions Under PCA .................................28
Appendix E: Resolution ..................................................................................................29
Appendix F: Compliance With Enforcement Actions Page Template ............................31
Appendix G: Sample Write-Ups for Compliance With Enforcement Actions Section of a Formal Written Communication ..................................................................................33
Appendix H: Abbreviations ..............................................................................................35
Appendix I: References ....................................................................................................36
I. Introduction

The OCC uses enforcement actions against banks to require a bank’s board of directors (board)\(^4\) and management to take timely actions to correct a bank’s deficient practices\(^5\) or violations (collectively, deficiencies). Enforcement actions against banks are more severe than matters requiring attention (MRA). Violations, concerns in MRAs, or unsafe or unsound practices may serve as the basis for an enforcement action against a bank.

Deficient practices are practices or lack of practices that\(^6\)

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

Clear communication between the OCC and a bank’s board and management is critical. The OCC uses formal written communications, including reports of examination (ROE) and supervisory letters, to document and communicate the OCC’s findings and conclusions from its supervisory review of a bank. Formal written communications may contain concerns in MRAs or citations of violations requiring corrective action. The actions that the board and management take or agree to take in response to violations and concerns in MRAs are factors in the OCC’s decision to pursue a bank enforcement action and the severity of that action. In some cases, it may be appropriate for the OCC to pursue an enforcement action against a bank before the issuance of an examination’s formal written communication to require correction of significant deficiencies as quickly as possible.

A bank’s board and management must correct deficiencies in a timely manner. The OCC expects a bank’s board to ensure compliance with bank enforcement actions within required time frames by

- holding management accountable for the bank’s deficiencies.
- directing management to develop and implement corrective actions.
- approving necessary changes to the bank’s policies, processes, procedures, and controls.
- establishing processes to monitor progress and verify and validate the effectiveness of management’s corrective actions.

The OCC’s policy is to identify deficient practices and violations in a timely manner and initiate bank enforcement actions to require corrective action well before deficiencies affect a bank’s

---

\(^4\) In the case of federal branches and agencies, the use of “board of directors and management” refers to federal branch or agency management.

\(^5\) Practices include a bank’s policies, procedures, processes, and controls.

\(^6\) Refer to the “Bank Supervision Process” booklet of the Comptroller’s Handbook.
financial condition or viability. The OCC’s short- and long-term strategy for a bank with deficiencies is an important factor in determining the type of bank enforcement action(s) to use. The strategy considers the immediate actions needed to address the bank’s deficiencies and what actions might be needed in the future if the deficiencies develop into more serious concerns (for example, deficiencies threatening the bank’s viability). Although the primary objective of bank enforcement actions is remediation of a bank’s deficiencies, bank enforcement actions also can enhance the OCC’s position for timely and orderly resolution or receivership to protect the Deposit Insurance Fund. The documentation of bank enforcement actions, a bank’s failure to comply with those actions, and the consequences of that failure are important components of the supervisory record to support more severe subsequent bank enforcement actions when necessary.

II. Types of Bank Enforcement Actions

Enforcement actions against banks can be either formal or informal. Enforcement actions against banks do not include restrictions imposed by the OCC in response to a bank’s licensing filing or by operation of law (for example, mandatory restrictions pursuant to prompt corrective action (PCA) or consequences of being in “troubled condition” under 12 CFR 5).

Informal Bank Enforcement Actions

The OCC typically first cites a violation or documents a concern in an MRA in a formal written communication to address a bank’s deficiencies. Examiners should consider an informal bank enforcement action when a bank’s condition is sound but deficiencies have not been corrected in a timely manner or escalation beyond the OCC’s citation of a violation or documentation of a concern in an MRA is otherwise warranted. The board’s agreement or acceptance of an informal bank enforcement action can be indicative of its commitment to correct identified deficiencies before they adversely affect the bank’s condition. Informal bank enforcement actions are typically not published or made available to the public.

Informal bank enforcement actions include

- all nonpublic bank enforcement actions:
  - Commitment letters.
  - Memorandums of understanding (MOU).
  - Individual minimum capital ratios (IMCR).
- operating agreements.8

---

7 Refer to the “Bank Supervision Process” booklet of the Comptroller’s Handbook for more information.

8 An operating agreement is a “written agreement” within the meaning of 12 USC 1818, which means that it is enforceable under 12 USC 1818. Only those operating agreements that do not relate to a bank’s licensing filing are bank enforcement actions. Operating agreements that are associated with or result from a bank’s licensing filing, while enforceable under 12 USC 1818, are not, however, bank enforcement actions for the purposes of this PPM.
• conditions imposed in writing within the meaning of 12 USC 1818.\textsuperscript{9}

**Formal Bank Enforcement Actions**

When a bank’s deficiencies are severe, uncorrected, repeat, unsafe or unsound, or negatively affect the bank’s condition, the OCC may use formal bank enforcement actions to support the agency’s supervisory objectives. Formal bank enforcement actions are typically published or made available to the public and, with the exception of Gramm–Leach–Bliley Act (GLBA) agreements pursuant to 12 CFR 5.39 and formal agreements, formal bank enforcement actions also are enforceable through the federal court system. In addition, violations of a formal bank enforcement action can provide the legal basis for CMP assessments.

Formal bank enforcement actions include

• all bank enforcement actions enforceable by the OCC in federal court:
  − Consent orders and cease-and-desist (C&D) orders.
  − Restitution orders (a type of consent or C&D order).
  − Capital directives.
  − PCA directives.
  − Safety and soundness orders issued under 12 CFR 30.
• formal agreements.
• GLBA agreements pursuant to 12 CFR 5.39 (regarding financial subsidiaries of national banks).
• CMPs (refer to PPM 5000-7).

Refer to appendixes A and B of this PPM for more information regarding informal and formal bank enforcement actions and appendix D for a detailed discussion of the mandatory and discretionary provisions of PCA.

Banks subject to certain formal bank enforcement actions (that is, C&D orders, consent orders, or formal agreements) are in “troubled condition,” as defined in 12 CFR 5.51, unless the OCC otherwise informs the bank in writing.\textsuperscript{10} Banks in troubled condition must provide written notice to the OCC before adding or replacing directors or senior executive officers and are subject to restrictions on golden parachute payments.\textsuperscript{11} Consult with the appropriate OCC legal staff in the appropriate District Counsel’s office (District Counsel) or the Bank Activities and

\textsuperscript{9} Only those conditions imposed in writing outside of an approval of a bank’s licensing filing are bank enforcement actions. Conditions imposed in an approval of a bank’s licensing filing are not bank enforcement actions and are not within the scope of this PPM.

\textsuperscript{10} A bank is also in “troubled condition” if it has a composite rating of 4 or 5 under the Uniform Financial Institutions Rating System or is informed in writing by the OCC that, based on information pertaining to the bank, the bank has been designated in “troubled condition.” Refer to 12 CFR 5.51.

\textsuperscript{11} For more information, refer to 12 CFR 5.51, “Changes in Directors and Senior Executive Officers of a National Bank or Federal Savings Association”; the “Changes in Directors and Senior Executive Officers” booklet of the *Comptroller’s Licensing Manual*; and 12 CFR 359, “Golden Parachute and Indemnification Payments.”
Structure Division for more information regarding the consequences of “troubled condition,”
changes in directors or senior executive officers, or golden parachute payments.

III. Determining the Appropriate Supervisory or Enforcement Response

Examiners should consider the following factors when determining the appropriate response to
a bank’s deficiencies. These factors do not represent an exhaustive list, and examiners may
consider additional factors when warranted:

- The bank’s condition as reflected by its composite and component CAMELS/ITCC\textsuperscript{12} or
  ROCA\textsuperscript{13} ratings.
- The bank’s risk profile, including trends.
- The nature, extent, and severity of the bank’s deficiencies.
- The extent of any unsafe or unsound practices.
- The board and management’s ability and willingness to correct deficiencies within an
  appropriate time frame.
- Potential adverse impact to bank customers, the Deposit Insurance Fund, or the public.
- The nature, extent, and severity of previously identified but uncorrected deficiencies.
- The bank’s progress in achieving compliance with any existing enforcement actions.

The severity and direction of the bank’s deficiencies, ratings, and level of risk are crucial factors
to consider when deciding between an informal and formal bank enforcement action when

- the bank exhibits significant deficiencies in its risk management systems, including policies,
  processes, and control systems.
- there is significant insider abuse.
- there are systemic or significant violations of laws or regulations.
- the board and management have disregarded, refused, or otherwise failed to correct
  previously identified deficiencies, including
  - noncompliance with an existing enforcement action.
  - failure to correct concerns communicated in MRAs.
  - failure to correct violations of laws or regulations.
- the board and management have refused or failed to satisfactorily maintain the bank’s books
  and records; have attempted to place unreasonable limitations on how, when, or where an

\textsuperscript{12} CAMELS integrates ratings from six component areas: capital adequacy, asset quality, management, earnings,
liquidity, and sensitivity to market risk. ITCC ratings stand for information technology, trust, consumer
compliance, and Community Reinvestment Act.

\textsuperscript{13} ROCA is the supervisory rating system for U.S. branches and agencies of foreign banking organizations and
stands for risk management, operational controls, compliance, and asset quality.
examination is conducted; or have imposed limits or restrictions on examiner access to the
bank’s personnel, books, or records.

While the presumption favors a formal bank enforcement action as described above, the OCC
exercises judgment based on the totality of the conduct and circumstances.

Pursuant to 12 USC 1818(s), the OCC is required to issue a C&D order in certain BSA cases.
Enforcement Policy,” and OCC Bulletin 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.”

When the bank fails to achieve compliance with an informal bank enforcement action, the OCC
should consider a formal bank enforcement action to address the outstanding deficiencies. When
the bank fails to achieve compliance with a formal bank enforcement action, examiners should
consider whether additional actions (for example, CMP assessments or other enforcement
actions against the board or management or taking a more severe formal enforcement action
against the bank) are appropriate. Under certain rare circumstances, the supervisory office may
consider replacing an existing bank enforcement action with a more focused or less severe bank
enforcement action when the bank’s condition, risk profile, and nature of deficiencies warrant.
Refer to the “Terminating a Bank Enforcement Action” section of this PPM for more
information.

1- and 2-Rated Banks

Deficiencies in a bank with a composite CAMELS or ROCA rating of 1 or 2 generally can be
addressed through the use of MRAs or citations of violations in a formal written
communication. A bank enforcement action may be warranted based on the severity of
deficiencies or the board and management’s failure to address previously identified deficiencies.
Enforcement actions against banks generally increase in scope and severity when the OCC has
low confidence in the board or management’s willingness or ability to correct deficiencies. The
decision to recommend stronger bank enforcement action is the supervisory office’s responsibility, and the type of enforcement action should be based on the bank’s ratings, the
deficiencies’ severity, the level of risk, and the board and management’s ability and willingness
to correct the deficiencies within an appropriate time frame.

3-Rated Banks

There is a presumption for use of a formal bank enforcement action for a 3-rated bank. The
presumption is particularly strong when

- the bank is deteriorating because of declining trends in financial performance or an
  increasing risk profile.

14 For purposes of this PPM, “supervisory office” refers to the examiner-in-charge, problem bank specialist,
assistant deputy comptroller, director, associate deputy comptroller, or deputy comptroller, as appropriate,
depending on the OCC business unit.
• the bank has a less than satisfactory management component rating (3 or worse).
• there is uncertainty as to whether the board and management have the ability and willingness to correct identified deficiencies within an appropriate time frame.

4- and 5-Rated Banks

While the board and management’s ability and willingness to correct deficiencies within an appropriate time frame is a factor in deciding the type of a bank enforcement action, the OCC has a presumption in favor of using a C&D order, a consent order, or a PCA directive, given the condition and high-risk profile of composite 4- and 5-rated banks.

Resolution

The OCC has the authority to place a Federal Deposit Insurance Corporation (FDIC)-insured bank into conservatorship or receivership when the bank is insolvent or has tangible equity capital of 2 percent or less. Under certain circumstances, the OCC may initiate resolution by placing a bank into receivership or conservatorship, or requiring its sale, merger, or liquidation before the bank becomes insolvent or has tangible equity capital of 2 percent or less.\(^\text{15}\) Refer to appendix E of this PPM for more information on resolution options.

IV. Decision Authority and OCC Legal Staff Responsibilities

The Comptroller has delegated to the Major Matters Supervision Review Committee or to the senior deputy comptrollers for bank supervision the primary responsibility to use the OCC’s enforcement authority to accomplish the OCC’s supervisory and enforcement objectives. In certain cases, senior deputy comptrollers re-delegate authority to initiate, negotiate, execute, modify, or terminate enforcement actions, including bank enforcement actions.

Supervision Review Committees

The OCC has supervision review committees (SRC) that, among other things, review or make enforcement decisions and promote consistent application of OCC policies. The supervisory office and assigned OCC legal staff are typically responsible for presenting recommendations regarding enforcement actions to the appropriate committee.

- **Major Matters Supervision Review Committee (MMSRC):** The MMSRC makes enforcement decisions on cases of heightened importance because of their visibility, policy sensitivity, involvement of multiple agencies, nature of the issues, or potential systemic impact.
- **Washington Supervision Review Committee (WSRC):** The WSRC reviews enforcement action recommendations within its authority and serves as an advisory committee for the appropriate senior deputy comptroller who makes the final decision for his or her cases or decides to refer the case to the MMSRC.

\(^{15}\) Refer to 12 USC 1821(c)(5).
• **District or Midsize Supervision Review Committees (DSRC or MSRC):** Each OCC district office and the Midsize Bank Supervision division has an SRC that reviews supervisory and enforcement action recommendations within its authority and serves as an advisory committee for the appropriate deputy comptroller, who makes the final decision for his or her cases or decides to refer the case to the WSRC or the MMSRC.

**OCC Legal Staff Responsibilities**

The OCC legal staff responsible for a case typically varies by the SRC review required or whether the case involves litigation. Generally, District Counsel are primarily responsible for cases that require DSRC or MSRC review, while the Enforcement and Compliance Division (E&C) has responsibility for cases that require MMSRC or WSRC review or litigation. In most cases, responsibility transfers as indicated in table 1.

<table>
<thead>
<tr>
<th>Type of bank matter</th>
<th>Responsible OCC legal counsel (generally)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMSRC</td>
<td>E&amp;C</td>
</tr>
<tr>
<td>WSRC</td>
<td>E&amp;C</td>
</tr>
<tr>
<td>DSRC or MSRC</td>
<td>District Counsel</td>
</tr>
</tbody>
</table>
| Case that begins with DSRC or MSRC, then goes to the MMSRC or WSRC or otherwise involves litigation | Begins with District Counsel, then transfers to E&C  
  • after referral to the MMSRC or WSRC, or  
  • before filing a notice of charges to commence litigation. |

If District Counsel is primarily responsible for a case that may need to be presented to the MMSRC or WSRC by E&C or in which there is a likelihood of litigation, then District Counsel should promptly notify and consult E&C early in the process, well before any SRC consideration.

District Counsel and E&C also consult with specialized counsel in certain types of cases (e.g., cases involving certain consumer laws, securities laws, or the Bank Secrecy Act) or when otherwise appropriate.

V. **Formal Investigations**

In most cases, documents and information may be obtained from the bank by the OCC pursuant to its examination authority. An order of investigation (OOI), however, may be appropriate when the OCC’s examination authority is not sufficient to obtain documents or other information needed to accomplish OCC objectives, including determining whether (or to what extent) there has been misconduct by or at a bank. For example, an OOI is generally appropriate when sworn testimony is needed, or when subpoenas are needed to obtain

---

16 OOI are conducted pursuant to 12 USC 481 (national banks), 12 USC 1464(d) (federal savings associations), 12 USC 1817(j), 12 USC 1818(n), 12 USC 1820(c), 12 USC 3102(b) (federal branches and agencies), 12 USC 3108(a) and (b) (federal branches and agencies), 12 USC 3110 (federal branches and agencies), 12 CFR 19.180–184 (national banks), and 12 CFR 112 (federal savings associations).
documents from sources outside the bank. The OOI is a supplement to, and not a replacement for, the OCC’s examination process.

Pursuant to an OOI, the OCC may issue subpoenas to obtain documents and sworn testimony. The OCC may issue document subpoenas to institution-affiliated parties and to third parties (i.e., individuals and entities not directly affiliated with the bank). The OCC may also issue subpoenas to obtain sworn testimony (under oath, transcribed by a court reporter) from institution-affiliated parties or other individuals, who may be subject to criminal penalties if they do not testify accurately and honestly. Pursuant to 12 CFR 19.181 (national banks) and 12 CFR 112.3 (federal savings associations), information and documents obtained or used in the OOI are confidential (i.e., nonpublic OCC information).

If the supervisory office determines that an OOI may be appropriate, it should consult with OCC legal staff. The supervisory office and OCC legal staff should consider the need for, scope of, and resource requirements for any investigation. If the supervisory office and OCC legal staff determine that there is a basis for initiating an OOI, the supervisory office (together with OCC legal staff) must obtain the necessary approval from the appropriate decision maker. Before opening an OOI that does not require presentation to the MMSRC or WSRC, the District Counsel should consult with the Director of E&C to ensure proper coordination of investigations.

Upon the initiation of an OOI, OCC legal staff and the supervisory office should prepare an investigative plan. Investigations should be conducted with a clear supervisory objective and a realistic strategy for achieving that objective. Accordingly, OOI investigative plans must focus on specific issues, describe investigatory steps, include time frames for completion, and be updated periodically as necessary. Investigations are often resource-intensive and require ongoing supervisory and legal attention. While the goal of investigations is to gain a complete understanding of the relevant conduct or transactions, investigations should nonetheless be conducted efficiently. Upon completion of an investigation, the supervisory office together with OCC legal staff must determine whether to recommend any enforcement action based on the findings to the appropriate decision maker and proceed accordingly. Finally, upon completion of an investigation, the supervisory office together with legal staff must seek approval from the appropriate decision maker to terminate the OOI.

VI. Content of Bank Enforcement Actions

Bank enforcement actions must address deficiencies documented in a related formal written communication or otherwise uncovered during an examination or investigation, as appropriate. Concerns in MRAs may be escalated into a bank enforcement action. Once the OCC determines which deficiencies must be addressed in the bank enforcement action, the enforcement action must

- identify the underlying basis for the enforcement action.
- specifically state any requirements placed on the bank and list any restrictions or limitations on the bank’s activities.
be explicit to guide the board’s or management’s corrective actions and facilitate OCC follow-up activities.

- assign time frames by which the board or management must act, complete any corrective actions, or be subject to restrictions or limitations on activities.

Bank enforcement actions should generally be drafted using standard introduction, closing, and other language provided by the OCC’s Director for E&C, but they must be appropriately tailored to address the specific deficiencies of the bank. Bank enforcement actions must be drafted by or in consultation with OCC legal staff.

**VII. Timeliness of Bank Enforcement Actions**

The OCC’s policy is to take bank enforcement actions as soon as practical, including during an examination if circumstances warrant. Whenever possible, the proposed enforcement action should be presented to the bank within 180 days of the start of a supervisory activity that results in any formal written communication that

- states that the bank is experiencing one or more of the significant deficiencies listed in the “Determining the Appropriate Supervisory or Enforcement Response” section of this PPM.
- assigns a composite CAMELS or ROCA rating of 3, 4, or 5.
- states that the bank is undercapitalized, significantly undercapitalized, or critically undercapitalized.
- states that an undercapitalized bank has failed to submit an acceptable capital restoration plan or has failed in some material respect to implement it.
- states that the bank is in noncompliance with the safety and soundness guidelines (12 CFR 30, appendix A).

Cases extending beyond these guidelines must be approved by the appropriate deputy comptroller and documented in the OCC’s supervisory information systems with supporting information.

Bank enforcement action recommendations based on facts gathered pursuant to an OOI should be presented to the appropriate SRC expeditiously upon completion of the investigative work. The investigative work is typically considered to be complete when the assigned legal and supervisory team has determined that it has accomplished the tasks set out in the investigation plan (e.g., completion of the last sworn statement, interview, or document review).

Cases involving unique circumstances, including those that entail coordination with other agencies, may add to the time needed to process a case or present a bank enforcement action recommendation to the appropriate SRC. The legal and supervisory team should account for and describe these unique circumstances in the OOI investigative plan.

**VIII. Follow-Up Activities**

The OCC’s timely assessment and written feedback on the bank’s progress toward compliance with a bank enforcement action are critical to helping the board and management understand the
requirements of the enforcement action and achieve timely compliance. The bank’s success or failure in complying with an enforcement action and the impact on the bank from continuation of the deficiencies should be thoroughly documented in the OCC’s supervisory information systems. The findings of the OCC’s assessment and any recommendation to take further action or modify the bank enforcement action must be presented to the appropriate SRC when required. Noncompliance with a bank enforcement action can support a more severe enforcement action and, in appropriate cases, resolution actions.

The OCC’s supervisory strategies for banks with enforcement actions must include plans for examiner follow-up. The plans must include activities to monitor progress and verify and validate the effectiveness of the board and management’s corrective actions. Plans must include the timing, expertise, and resource requirements.

Examiners must perform the first assessment of a bank’s compliance with an enforcement action within 180 days of the date the enforcement action was executed. While the enforcement action remains outstanding, examiners must assess compliance with the enforcement action at least once within the bank’s supervisory cycle. The timing of follow-up activities should be aligned to corrective action due dates and the bank’s action plans.

The OCC’s bank enforcement action follow-up activities include verification and validation.

- **Verification** is the process by which examiners review the bank’s documentation and confirm that the board and management completed the required corrective actions.
- **Validation** is the process by which examiners confirm the effectiveness and sustainability of corrective actions.

**IX. Assessing Compliance With Bank Enforcement Actions**

Upon completing follow-up activities, examiners must determine whether the bank has met the requirements of each article and designate the article as “in compliance” or “not in compliance.”

When an article is designated in compliance, the bank has adopted, implemented, and adhered to all of the corrective actions set forth in the article; the corrective actions are effective in addressing the deficiencies; and the OCC has verified and validated the corrective actions. An article must not be deemed in compliance simply because the board and management have made progress or a good faith effort toward complying with the article. Articles that are in compliance can fall out of compliance at any time the bank enforcement action remains outstanding.

All other articles are designated as not in compliance, including

- articles that are past due, including when the board and management have failed to
  - adopt policies, procedures, and systems required by the article within required time frames.
  - comply with immediately effective requirements.
  - cease activities prohibited by the article.
implement or adhere to corrective actions required by the article, including when
examiners determine during validation that corrective actions are not effective or
sustainable.

- articles that are pending validation (that is, examiners verified that management
implemented the corrective actions, but insufficient time has passed for the bank to
demonstrate sustained performance under the corrective actions, examiners have not
validated the sustainability of the corrective actions, or examiners determine additional
testing is warranted).

X. Communicating Bank Enforcement Action Compliance

Examiners must provide written communication to the bank after completing verification or
validation activities, or in response to a bank’s submission or request, as described in this
section. Formal written communications that discuss compliance with a bank enforcement
action must include a “Compliance With Enforcement Actions” section. Refer to appendixes F
and G of this PPM for full requirements, a template, and a sample write-up. This section should
be tailored to the scope of the follow-up activity and must include the following:

- A table that states the status (that is, in compliance or not in compliance) of each actionable
  article, as appropriate.
- A write-up for each actionable article that includes
  - a summary of the article’s requirements.
  - status of the actions required.
  - additional actions required, if applicable.
  - commitment, if applicable.

Write-ups for articles that are in compliance are optional when the article was also
communicated as “in compliance” in a previous written communication, unless material
information regarding the article or management’s or the board’s actions have changed since the
prior communication.

The annual ROE for banks under continuous supervision\(^1\) may summarize the status of bank
enforcement action articles and reference relevant formal written communications that occurred
throughout the supervisory cycle. Write-ups for articles should be included if the article’s status
has changed since the prior formal written communication.

Bank Submissions and Requests

Bank enforcement actions generally require the bank to periodically submit a progress report,
action plan, or other documentation (collectively, submissions) to the OCC. Examiners must
review and respond to the bank’s submission within 30 days of receipt or inform the bank in
writing of the date that examiners will review the submission.

\(^1\) Banks under continuous supervision include midsize and large banks, and some large community banks. Banks
under continuous supervision receive supervisory letters communicating the results of targeted examinations
throughout the supervisory cycle and an annual ROE that aggregates the results of all supervisory activities and
conveys the bank’s CAMELS or ROCA ratings.
Bank enforcement actions may include a provision whereby the board may request an extension of a time frame or waiver or suspension of provision(s) in the enforcement action. Requests must be submitted in writing with facts to support the request. Extensions must be requested in advance of the corrective action due date. The OCC’s response must be in writing, and support for decisions must be documented in the OCC’s supervisory information systems. The length of time a bank takes to achieve compliance with all provisions of an existing bank enforcement action may be a factor in the OCC’s consideration of any future actions.

XI. Terminating a Bank Enforcement Action

A bank enforcement action should not be terminated unless

- the bank is in compliance with all articles of the enforcement action,
- the OCC determines that articles deemed “not in compliance” have become outdated or irrelevant to the bank’s current circumstances, or
- the OCC incorporates the articles deemed “not in compliance” into a new action.

Escalation is the process of terminating an existing bank enforcement action and replacing it with a more comprehensive or severe action (for example, from an MOU to a formal agreement or from a formal agreement to a consent order). Considerations for determining whether to escalate a bank enforcement action include the

- bank’s level of compliance with an existing action.
- overall condition of the bank.
- direction of risk profile.
- board and management’s ability and willingness to correct deficiencies within an appropriate time frame.
- extent and severity of the deficiencies.
- nature, extent, and severity of new deficiencies identified after issuing the existing action.
- impact or potential impact to bank customers, the Deposit Insurance Fund, or the public.

Refer to the “Determining the Appropriate Supervisory or Enforcement Response” section of this PPM for more information regarding which type of bank enforcement action may be appropriate.

Additionally, if the bank has failed to achieve compliance with a formal bank enforcement action, examiners should consider additional actions, such as CMP assessments or other enforcement actions against the board or management, enforcement of the action in federal court, or the commencement of a new bank enforcement action that, in certain cases, includes a requirement for the sale, merger, or voluntary liquidation of the bank.

There may be some limited exceptions in which replacing a bank enforcement action with a less severe or less comprehensive action may be appropriate. This may be appropriate when the bank’s condition and risk profile have significantly improved and the severity of the existing enforcement action is inconsistent with the nature and extent of the bank’s condition, risk profile, and deficiencies.
The decision to terminate or replace a bank enforcement action follows the same review process through an SRC as for new enforcement actions. Refer to the “Decision Authority and OCC Legal Staff Responsibilities” section of this PPM for more information on SRCs.

XII. Documentation in OCC Supervisory Information Systems

The consistent administration of the OCC’s enforcement action documentation is important. The supervisory office must maintain accurate records of OCC enforcement actions against banks. This includes recording and maintaining actions, status, financial payment information (if applicable), relevant tracking dates, and supporting documents in the appropriate supervisory information systems. Supervisory offices must follow established procedures for entering, tracking, and closing bank enforcement actions and documenting supervisory activities related to bank enforcement action follow-up in the OCC’s supervisory information systems.

The OCC’s supervisory records must accurately reflect the efforts of the board and management to resolve deficiencies and the OCC’s supervisory activities or actions to ensure resolution. The OCC’s supervisory information systems must include the following relevant supporting documentation:

- The executed enforcement action document(s).
- The decision to initiate, modify, or terminate the enforcement action, including any SRC memorandums and other supporting decision documents.
- Relevant internal correspondence, correspondence with the bank (and, if applicable, documentation of the bank’s receipt of correspondence), and correspondence with other agencies (if applicable).
- The nature and extent of corrective actions, including who completed them and when they were completed.
- A conclusion about the effectiveness of the board and management’s corrective actions.
- A description of the actions examiners have taken to follow up on management’s or the board’s corrective actions.
- Details (for example, description, completion time frames, and names of responsible parties) of any additional corrective actions the board or management must complete.
- Supervisory actions resulting from the OCC’s follow-up activities (e.g., proposed changes to or termination of enforcement actions; strategy changes; CAMELS, ROCA, or specialty area rating changes; risk assessment system changes; and written communications to the bank).
XIII. Public Disclosure of Bank Enforcement Actions

The OCC is required to publish and make available to the public certain final enforcement actions against banks, including consent orders, C&D orders, restitution orders, formal agreements, capital directives, PCA directives, safety and soundness orders, CMPs, and any termination or modification of such actions. The OCC also makes available to the public GLBA agreements, conditions imposed in writing, and operating agreements. In addition, notices of charges are typically posted on the OCC’s website. The OCC may, at its discretion, choose not to publish a particular action or to delay publication under exceptional circumstances.18

The OCC’s Public Affairs office issues a monthly news release listing recent public enforcement actions and terminations, including public bank enforcement actions. The listing includes the name of the bank, the type of action (including notices of charges), and the date of the action. The monthly news release is available in the “News Releases” section of the OCC’s website. Published bank enforcement actions, including published notices of charges, are also posted and available via a searchable “Enforcement Actions” page on the OCC website. Disclosures related to enforceable operating agreements and conditions imposed in writing are not included in the monthly enforcement actions news release but can be found in the “Interpretations and Actions” section of the OCC’s website.

In certain cases, the OCC may issue a news release for an enforcement action when appropriate. Examiners should consult with Public Affairs and OCC legal staff in these instances.

Disclosures by Banks

Disclosures described in the preceding paragraphs refer only to the OCC’s required or discretionary disclosures. Banks are not permitted to disclose the existence of any nonpublic informal action, any potential (non-final) enforcement action (including any 15-day letter or proposed, unexecuted consent order), or any information obtained in the course of a formal investigation (including subpoenas) to a party other than its attorney without OCC authorization following a request submitted in accordance with 12 CFR 4, subpart C. Nothing in this paragraph, however, is intended to relieve any bank, or, when applicable, its holding company, of independent obligations to make required disclosures pursuant to laws, regulations, or other obligations. A bank seeking to make a required disclosure pursuant to an independent obligation must submit a request to the OCC in accordance with 12 CFR 4, subpart C.

All public bank enforcement actions, operating agreements, and conditions imposed in writing are considered to be public at the time they are executed (i.e., signed by all parties, including the appropriate OCC official), unless the OCC otherwise notifies the banks. Banks may, therefore, disclose executed documents described in this paragraph without further action by the OCC (i.e., prior to publication by the OCC).

For further information regarding OCC enforcement actions against banks, please contact E&C at (202) 649-6200 or Special Supervision at (202) 649-6450.

---

18 Refer to 12 USC 1818(u).
Toney M. Bland
Senior Deputy Comptroller for Midsize and Community Bank Supervision

Grace E. Dailey
Senior Deputy Comptroller for Bank Supervision Policy and Chief National Bank Examiner

Grovetta N. Gardineer
Senior Deputy Comptroller for Compliance and Community Affairs

Morris R. Morgan
Senior Deputy Comptroller for Large Bank Supervision

Bao Nguyen
Acting Senior Deputy Comptroller and Chief Counsel
Appendix A: Informal Enforcement Actions Against Banks

Commitment letter (not public): A document signed by the board on behalf of the bank and acknowledged by an authorized OCC official, making specific written commitments to take corrective actions in response to the bank’s deficiencies. The document may be drafted by either the OCC or the bank. A commitment letter is not a binding legal document (that is, the OCC cannot enforce compliance in federal court or assess CMPs for noncompliance); a board’s failure to honor the commitments, however, may provide strong evidence of the need for a formal bank enforcement action.

Conditions imposed in writing (public if explicitly made enforceable under 12 USC 1818): A “condition imposed in writing” within the meaning of 12 USC 1818 is imposed on a bank by the supervisory office in connection with an action on an application, notice, or other request. Examples of conditions imposed in writing include conditions imposed by the OCC when communicating a written determination of no supervisory objection or when granting a bank’s request to terminate a bank enforcement action. Conditions imposed in writing may be imposed to protect the safety and soundness of the bank, prevent conflicts of interest, ensure that the bank provides consumer protections, ensure that the OCC’s approval is consistent with laws or regulations, or provide for other supervisory or policy considerations. Conditions imposed in writing remain in effect until the OCC removes them. Any violations of conditions imposed in writing can provide the legal basis for additional enforcement actions, including a CMP assessment.

Conditions imposed by the OCC’s Licensing Division in association with or resulting from a bank’s licensing filing, although typically enforceable under 12 USC 1818, are not bank enforcement actions and are not within the scope of this PPM.

Individual minimum capital ratios (not public): The OCC is authorized under 12 USC 1464(s)(2), 12 USC 3907, and 12 CFR 3, subpart H, to establish higher IMCRs for a bank in light of its particular circumstances. When the OCC determines that higher capital ratios are necessary, it sends the bank a notice of intent to establish higher minimum capital ratios (IMCR notice). The IMCR notice includes the proposed capital ratios, the date they must be reached, and an explanation of why the OCC considers the proposed ratios necessary or appropriate for the bank. The bank may provide a written response within 30 days of the IMCR notice, unless the OCC specifies a shorter time frame. The bank’s response should include any matters the board and management believe the OCC should consider in deciding whether to establish an IMCR, what management or the board believe the IMCR should be, and when the bank should achieve the ratios. The bank’s failure to respond within the required time frame is considered a waiver to any objection to the proposed IMCR. The OCC makes its decision after the close of the response period and notifies the bank of its decision in writing using a notification of establishment of higher capital ratios (IMCR decision notification). The IMCR decision notification includes an explanation of the OCC’s decision and may require the bank to develop and submit to the OCC an acceptable plan to reach the higher minimum capital ratios.
The establishment of an IMCR does not affect a bank’s PCA capital category. If a bank fails to maintain its capital ratios above the higher minimums established in the IMCR, the OCC may issue a capital directive requiring the bank to submit and adhere to an acceptable plan to achieve or maintain its required capital levels. Additionally, the OCC may deem a bank’s failure to maintain capital ratios above the IMCR an unsafe or unsound practice within the meaning of 12 USC 1818.19

Memorandum of understanding (not public): A bilateral document between a bank and the OCC that looks similar to a formal OCC enforcement action in form and content. An MOU is drafted by the OCC. Like a commitment letter, an MOU is not a binding legal document, but a board’s failure to honor an MOU may provide strong evidence of the need for a formal bank enforcement action.

Operating agreement (public if made explicitly enforceable under 12 USC 1818): A bilateral document signed by the board on behalf of a bank and an authorized OCC official. Operating agreements typically specify that they are “written agreements” within the meaning of 12 USC 1818 (that is, enforceable operating agreements). In such cases, violations of an operating agreement can provide the legal basis for additional enforcement actions, including CMP assessments. Unlike a C&D or consent order, operating agreements are not enforceable through the federal court system.

Operating agreements executed by the OCC’s Licensing Division in association with or resulting from a bank’s licensing filing are not bank enforcement actions and are not within the scope of this PPM.

Notice of deficiency issued under 12 CFR 30 (not public): Pursuant to 12 USC 1831p-1 and 12 CFR 30, the OCC may issue a notice of deficiency when a bank fails to comply with any established safety and soundness standard in 12 CFR 30. The notice of deficiency requires the bank to submit to the OCC a safety and soundness plan describing the steps the bank will take to correct the deficiency, including the time frame within which the bank will take those steps. The bank generally has 30 days to provide its safety and soundness plan; under certain circumstances, the OCC may shorten the time frame for the bank’s response. If the bank fails to submit an acceptable plan or fails in any material respect to implement an approved plan, the OCC must, by order, require the bank to correct the deficiencies, and the OCC may, by order, require the bank to take any other action provided in 12 USC 1831p-1(e)(2)(B). Refer to appendix B of this PPM for more information regarding safety and soundness orders.

19 Refer to 12 USC 3907(b)(1) and 1464(s)(3).
Appendix B: Formal Enforcement Actions Against Banks

Many formal bank enforcement actions below are designated as “public” because they are generally required to be published or made available to the public. 12 USC 1818(u), however, provides the OCC with the authority to delay or withhold publication under certain exceptional circumstances.

**Capital directive (public):** Pursuant to 12 USC 3907 and 12 CFR 3, the OCC may issue a Capital directive when a bank fails to achieve or maintain capital at or above the minimum ratios required by 12 CFR 3, subparts B or H; a written agreement; or a condition for approval of an application. A capital directive may require the bank to achieve its minimum capital requirement by a specified date, submit and adhere to an acceptable capital plan, and take other actions to achieve the required capital ratios. The OCC sends the bank a notice of intent to issue a directive, which includes reasons for the proposed directive and proposed contents. The bank generally has 30 days to provide a written response to the notice, though the OCC can shorten the time period for the bank’s response under certain circumstances. The bank’s response should state any reasons the bank believes a directive should not be issued, propose alternative contents for the directive, and include any other matters that the bank would like the OCC to consider in deciding whether to issue a directive or revise the directive’s contents. The bank’s failure to respond within the required time frame is considered a waiver of any objection to the proposed capital directive. The OCC makes its decision after receiving a response or after the close of the response period.

A capital directive has essentially the same force and effect as a C&D order. Violations of a capital directive can provide the legal basis for assessing CMPs against the bank and its institution-affiliated parties under 12 USC 1818(i) or 12 USC 3909(d). A capital directive may also be enforced through application to a U.S. District Court. Unlike C&D orders, a failure to meet or a willful violation of a capital directive is not itself grounds for receivership.

Capital directives are rarely used because most banks with deficient capital have other deficiencies that also need to be addressed, and they are addressed through other formal bank enforcement actions. When capital adequacy is the overriding consideration and other deficiencies do not need to be addressed through a formal bank enforcement action, capital directives can be useful.

**Cease-and-desist order (public):** A final order issued pursuant to 12 USC 1818(b) that may be issued when a bank engages in an unsafe or unsound practice or violates a law, rule, regulation, condition imposed in writing,20 or written agreement (for example, an operating agreement made enforceable under 12 USC 1818, or a formal agreement). In addition to requiring a bank to cease and desist from the unsafe or unsound practice or violation and to take affirmative action to correct or remedy any conditions resulting from any violation or practice, a C&D order may

---

20 A “condition imposed in writing” under 12 USC 1818 is defined as any condition imposed in writing by a federal banking agency in connection with any action on any application, notice, or other request by the depository institution or institution-affiliated party. This definition includes conditions imposed on a bank by the supervisory office as well as conditions imposed by the OCC’s Licensing Division.
require a bank to make restitution or provide reimbursement (i.e., restitution orders), restrict asset growth, dispose of a loan or other asset, rescind an agreement or contract, employ qualified officers or employees, or take other actions the OCC determines to be appropriate. A C&D order may also place limitations on a bank’s activities or functions. A C&D order is imposed on an involuntary basis after the issuance of a notice of charges, a hearing, a recommended decision by an administrative law judge, and a final decision and order by the Comptroller. The Comptroller’s decision to issue a C&D order in this manner is appealable to a U.S. Court of Appeals (either the D.C. Circuit or the circuit in which the home office of the bank is located). The OCC may enforce a C&D order through application to a U.S. District Court. Violations of a C&D order can provide the legal basis for additional enforcement actions, including CMPs. A willful violation of a final C&D order is itself grounds for receivership.21

Restitution order (public): A restitution order is a type of C&D order, authorized under 12 USC 1818(b)(6), that can be used to require a bank to take affirmative action to correct or remedy any conditions resulting from any violation or unsafe or unsound practice, including a requirement to make restitution (or provide reimbursement, indemnification, or guarantee against loss) if the bank was unjustly enriched in connection with the violation or practice, or the violation or practice involved a reckless disregard for the law, any applicable regulations, or prior order.

Civil money penalties (public): Refer to PPM 5000-7.

Consent order (public): Aside from its title, a consent order is identical in form and legal effect to a C&D order. A consent order, however, is issued with the consent of the bank’s board.

Temporary cease-and-desist order (not public except for the related notice of charges): A temporary C&D order is issued by the OCC pursuant to 12 USC 1818(c) following the filing of a notice of charges seeking a C&D order. The OCC may issue a temporary C&D order to a bank when the violation or unsafe or unsound practice described in the notice of charges, or the continuation of the violation or practice, is likely to cause the bank’s insolvency, cause significant dissipation of the bank’s assets or earnings, weaken the bank’s condition, or otherwise prejudice the interests of the bank’s depositors before the completion of the proceedings resulting from the notice of charges. A temporary C&D order may also be imposed if the notice of charges specifies a bank’s books and records are so incomplete or inaccurate that the OCC is unable, through the normal supervisory process, to determine the financial condition of the bank or the details or purpose of any transaction(s) that may have a material effect on the financial condition of the bank, or if the notice of charges specifies that any person has engaged in certain false advertising, misuse of FDIC names, or misrepresentations to indicate insured status as described in 12 USC 1828(a)(4). Although a temporary C&D order may be challenged in U.S. District Court within 10 days of issuance, it is effective upon issuance and remains effective and enforceable, unless set aside, limited, or suspended by the court, until a final C&D order is in place or the OCC dismisses the charges in the notice. Violations of a temporary C&D order can provide the legal basis for the assessment of CMPs.

21 Refer to 12 USC 1821(c)(5)(D), “Grounds for Appointing Conservator or Receiver.”
Formal agreement (public): A formal agreement, a “written agreement” within the meaning of 12 USC 1818, is a bilateral document signed by an authorized OCC official and the board on behalf of a bank. Violations of a formal agreement can provide the legal basis for additional enforcement actions, including CMP assessments. Formal agreements are not enforceable through the federal court system.

Gramm–Leach–Bliley Act agreements (national banks only, public): An agreement between a national bank and the OCC pursuant to 12 USC 24a(e)(2) and (3) and 12 CFR 5.39(j)(1)(ii) and (iii). A national bank that controls or holds an interest in a financial subsidiary must execute a GLBA agreement with the OCC within 45 days after receiving notice that

- the national bank or any of its depository institution affiliates are not well capitalized or well managed,
- the aggregate consolidated financial subsidiary assets exceed the limits of 12 CFR 5.39(g)(2),
- the national bank’s accounting treatment for any financial subsidiary does not comply with the standards set forth in 12 CFR 5.39(h)(1) and (2),
- the national bank’s procedures for identifying and managing financial and operational risks within the bank and the financial subsidiary do not adequately protect the bank from such risks, or
- the national bank’s policies and procedures to preserve the separate corporate identity and limited liability of the bank and the financial subsidiaries are not reasonable.

A GLBA agreement requires the national bank to comply with certain prudential requirements and may include limitations on the conduct or activities of the national bank or any subsidiary of the national bank as the OCC determines to be appropriate. If the national bank fails to correct the conditions giving rise to the notice within 180 days after receipt, the OCC may require the national bank to divest control of any financial subsidiary.

Prompt corrective action directive (FDIC-insured banks only, public): FDIC-insured banks are subject to mandatory and discretionary restrictions and actions depending upon the bank’s PCA capital category. Mandatory restrictions and actions are effective when the bank is notified or is deemed to have notice of its PCA capital category. The OCC imposes discretionary restrictions and actions on the bank through the issuance of a PCA directive. Discretionary restrictions include requiring recapitalization, restricting affiliate transactions, restricting interest rates, requiring sale of voting shares, further restricting asset growth, restricting activities, requiring election of new board members, requiring dismissal of directors or officers, requiring new senior executive officers, prohibiting deposits from correspondent banks, requiring divestiture of subsidiaries, or taking any other action that the OCC determines will resolve the bank’s problems at the least possible long-term cost to the Deposit Insurance Fund.

---

22 “Well capitalized” and “well managed” are defined in 12 CFR 5.39. For purposes of 12 CFR 5.39, “well managed” generally means that the bank has composite and management ratings of 1 or 2.

The OCC first issues a notice of intent to issue a PCA directive to the bank, unless the OCC finds it necessary to issue a PCA directive, which is immediately effective, without providing such notice. The bank is given an opportunity to respond to the notice and explain why the proposed PCA directive is not necessary, suggest any modifications to the proposed PCA directive, or provide any other relevant information to support its position. After considering the bank’s response, the OCC may issue the PCA directive as proposed or in modified form, determine that no action is necessary, or seek more information from the bank. A PCA directive essentially has the same force and effect as a C&D order. A PCA directive may also be enforced through application to a U.S. District Court.

For banks that are in the undercapitalized, significantly undercapitalized, or critically undercapitalized categories, the supervisory office should consider using a PCA directive. A PCA directive can enhance the OCC’s use of resolution options later because failure to become adequately capitalized when subject to a PCA directive is a ground for receivership.24 Similarly, PCA directives may be appropriate when the need for prompt action is present. Refer to appendix D for more information on mandatory and discretionary actions under PCA.

**Safety and soundness order (public):** If a bank fails to submit or implement an acceptable safety and soundness plan pursuant to 12 CFR 30, the OCC must require the bank to correct the deficiencies and may require the bank to take other actions under 12 USC 1831p-1(e)(2)(B) until the deficiency has been corrected. The OCC requires the correction of deficiencies and any other actions using a safety and soundness order. The OCC must also take certain additional actions against a bank that has not corrected a deficiency if the bank has experienced extraordinary growth over the past 18 months, has commenced operations within the past 24 months, or has undergone a change in control.

If circumstances warrant, the OCC may issue a safety and soundness order that is immediately effective. Otherwise, the process for issuing a safety and soundness order under 12 CFR 30.5 begins with the issuance of a notice of intent to issue a safety and soundness order. The notice identifies the safety and soundness deficiencies and describes the proposed actions that would be included in the order and the time frame for complying with the proposed actions. The bank is given an opportunity to respond to the notice by explaining why the proposed order is not necessary or offering suggested modifications to the proposed order. After considering the response, the OCC may issue a safety and soundness order or determine that no action is necessary. A safety and soundness order has essentially the same force and effect as a C&D order. A safety and soundness order may also be enforced through application to a U.S. District Court. Unlike C&D orders, a willful violation of a safety and soundness order is not itself grounds for receivership.

Unlike PCA directives and capital directives, a safety and soundness order allows the OCC to require a bank to address deficiencies in its operations regardless of the bank’s capital levels. Use of a safety and soundness order may be considered when a bank has serious systemic weaknesses resulting in the failure to meet one or more of the safety and soundness standards set forth in

---

24 Refer to 12 USC 1821(c)(5)(K)(ii).
12 CFR 30, but is not undercapitalized for PCA purposes and is not subject to an existing formal enforcement action that addresses the deficiency.
Appendix C: Bank Enforcement Action Processes and Time Frames

This appendix outlines the general process and timelines by type of enforcement action. Refer to the “Decision Authority and OCC Legal Staff Responsibilities” and “Timeliness of Bank Enforcement Actions” sections of this PPM for more information.

Time frames marked with an asterisk (*) in this appendix are set forth in statute or regulation.

<table>
<thead>
<tr>
<th>Enforcement action types</th>
<th>Process and time frames</th>
</tr>
</thead>
</table>
| Capital directive        | • The supervisory office should provide a notice of intent to issue a capital directive to the bank within 30 days of the OCC’s final decision to issue the notice.  
                              • The bank has 30 days* after receiving the notice to respond to the OCC, unless the OCC specifies a shorter time frame.  
                              • The OCC should consider any response from the bank, make a final decision whether to issue the directive, and provide any directive to the bank within 30 days of the expiration of the response period. If the OCC decides not to issue a directive, the OCC will notify the bank in writing. |
| C&D order                | • The supervisory office should provide the proposed enforcement action to the board within 30 days of the OCC’s final decision to take the enforcement action.  
                              • The OCC should obtain signatures from the board and execute the document within 30 days following delivery of the copy of the enforcement action to the board.  
                              • If the board does not execute the proposed enforcement action within 30 days following delivery, the OCC should expeditiously prepare and serve on the bank a notice of charges for a C&D order. |
| Consent order            | • The bank or the OCC drafts the commitment letter within 30 days of the OCC’s final decision to seek execution of a commitment letter.  
                              • The board should sign the commitment letter and the supervisory office should acknowledge the board’s commitment within 30 days of the OCC’s final decision to require the board to sign the commitment letter. |
| Conditions imposed in writing | • The bank provides an application, notice, or other request to the supervisory office that is not a licensing filing under 12 CFR 5.  
                                  • The supervisory office should provide the conditions imposed in writing to the bank within 30 days after the OCC makes a final decision to impose a condition in writing in connection with its action on the bank’s application, notice, or other request. |
| Formal agreement         | • The supervisory office should provide the proposed enforcement action to the board within 30 days of the OCC’s final decision to take the enforcement action.  
                              • The OCC should obtain signatures from the board and execute the document within 30 days following delivery of the copy of the enforcement action to the board.  
                              • If the board does not execute the proposed enforcement action within 30 days following delivery, the OCC should expeditiously prepare and serve on the bank a notice of charges for a C&D order. |
| GLBA agreement (national banks only) | • The OCC must notify a national bank that it does not continue to meet the relevant qualifications in 12 CFR 5.39(g) and safeguards in 12 CFR 5.39(h).  
                                  • Pursuant to 12 CFR 5.39(j), the bank must execute the agreement within 45 days* of the OCC’s notice that the bank does not meet the relevant qualifications and safeguards, unless the OCC extends the time frame. The following are guidelines for meeting this time frame: |
<table>
<thead>
<tr>
<th>Enforcement action types</th>
<th>Process and time frames</th>
</tr>
</thead>
</table>
|                          | - The supervisory office should provide the proposed agreement to the bank within 30 days after the OCC's decision to take the enforcement action.  
- The OCC should obtain signatures from the board and execute the document within 15 days following delivery of the copy of the agreement to the bank, unless the OCC permits additional time. |
| IMCR                     | - The supervisory office should provide a notice of intent to establish an IMCR to the bank within 30 days of the OCC's final decision to issue the notice of intent.  
- The bank has 30 days* after receiving the notice of intent to respond to the OCC, unless the OCC specifies a different time frame.  
- The OCC should make its decision whether to establish an IMCR and notify the bank in writing of its decision within 30 days after expiration of the response period. |
| Operating agreement      | - The supervisory office should provide the proposed enforcement action to the board within 30 days of the OCC's final decision to take the enforcement action.  
- The OCC should obtain signatures from the board and execute the document within 30 days following delivery of the copy of the enforcement action to the board. |
| MOU                      | - The OCC may immediately issue a PCA directive or issue a notice of intent to issue a PCA directive.  
- If the supervisory office finds it necessary to immediately issue a directive, the supervisory office should provide the PCA directive to the bank within 14 days of the OCC’s final decision to immediately issue the directive.  
- If the OCC issues a notice of intent, the supervisory office should provide the notice to the bank within 30 days of the OCC’s final decision to issue a notice of intent.  
- The bank may file a written response to the notice within the time period set by the OCC. The date must be at least 14 calendar days* from the date of the notice unless the OCC determines that a shorter time frame is appropriate.  
- The OCC should consider any response from the bank, make a final decision whether to issue the directive, and provide any directive to the bank within 30 days of the expiration of the response period. If the OCC decides not to issue a directive, the OCC will notify the bank in writing. |
| Notice of deficiency issued under 12 CFR 30 | - The supervisory office should provide a notice of deficiency to the bank within 30 days of the OCC’s final decision to issue the notice.  
- The bank must submit a safety and soundness plan to the OCC within 30 days* after receiving the notice of deficiency, unless the OCC specifies a different time frame.  
- The supervisory office must notify the bank whether the plan has been approved or seek more information regarding the plan within 30 days* after receiving the plan, unless the OCC extends the approval time frame. |
| Safety and soundness order | - The OCC may immediately issue a safety and soundness order or issue a notice of intent to issue a safety and soundness order.  
- If the supervisory office finds it necessary to immediately issue a safety and soundness order, the supervisory office should provide the order to the bank within 30 days of the OCC’s final decision to issue the order. |
<table>
<thead>
<tr>
<th>Enforcement action types</th>
<th>Process and time frames</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>− If the OCC issues a notice of intent, the supervisory office should provide the notice to the bank within 30 days of the OCC’s final decision to issue a notice of intent.</td>
</tr>
<tr>
<td></td>
<td>• The bank may file a written response to the notice within the time period set by the OCC. Such a response must be received by the OCC within 14 calendar days* from the date of the notice, unless the OCC specifies a different time frame is appropriate.</td>
</tr>
<tr>
<td></td>
<td>• The OCC should consider any response from the bank, make a final decision whether to issue the order, and provide any order to the bank within 30 days of the expiration of the response period. If the OCC decides not to issue an order, the OCC will notify the bank in writing.</td>
</tr>
<tr>
<td>Temporary C&amp;D order</td>
<td>• The OCC should serve a notice of charges and temporary C&amp;D order on a bank within 21 days of the OCC’s final decision to issue a temporary C&amp;D order to the bank.</td>
</tr>
<tr>
<td></td>
<td>• Within 10 days* after the OCC serves the temporary C&amp;D on the bank, the bank may apply for an injunction in U.S. District Court to set aside, limit, or suspend the temporary C&amp;D.</td>
</tr>
</tbody>
</table>
Appendix D: Mandatory and Discretionary Provisions Under PCA

This appendix summarizes the mandatory and discretionary actions under PCA, which are triggered by a bank’s PCA capital category. This appendix is not an exhaustive list of supervisory actions under PCA. For more information on PCA and its mandatory and discretionary supervisory actions, refer to 12 USC 1831o, 12 CFR 6, and OCC Bulletin 2018-33, “Prompt Corrective Action: Guidelines and Rescissions.” For purposes of this appendix, the term “bank” refers only to “insured depository institutions” as defined in 12 USC 1813(c)(2).

<table>
<thead>
<tr>
<th>PCA category</th>
<th>Applicable PCA provisions</th>
</tr>
</thead>
</table>
| Well capitalized                     | If the bank would be undercapitalized after making the payment, then  
• capital distributions (cash or certain other distributions) restricted.  
• management fees restricted. |
| Adequately capitalized               | Same as well capitalized banks, plus  
• brokered deposits restricted.\(^a\)                                                                                                                                  |
| Undercapitalized                     | Same as adequately capitalized banks, plus  
• restrictions on asset growth, acquisitions, new branches, and new lines of business.  
• bank must submit an acceptable Capital Restoration Plan (CRP) to the OCC within 45 days of the date the bank was notified of its undercapitalized status.  
• discretionary application of certain restrictions otherwise applicable only to significantly undercapitalized banks. |
| Significantly undercapitalized banks and undercapitalized banks that have failed to submit an acceptable CRP | Same as undercapitalized banks, plus  
• restrictions on senior executive officer compensation.  

The OCC shall also take one or more of the following actions:  
• Require recapitalization.\(^b\)  
• Restrict affiliate transactions.\(^b\)  
• Restrict interest rates on deposits.\(^b\)  
• Further restrict asset growth or require the bank to reduce assets.  
• Require the bank to alter, reduce, or terminate activities.  
• Require the bank to improve management by electing new directors, dismissing directors or senior executive officers, or requiring qualified senior executive officers.  
• Prohibit the bank’s acceptance of deposits from correspondent banks.  
• Require certain divestitures of subsidiaries.  
• Require the bank to take any other action the OCC determines will resolve the bank’s problems at the least possible long-term cost to the Deposit Insurance Fund better than any of the actions described here.  
• Require certain divestitures of subsidiaries.  
• Require the bank to take any other action the OCC determines will resolve the bank’s problems at the least possible long-term cost to the Deposit Insurance Fund better than receivership or conservatorship.  
• restrictions on payments of principal or interest on the bank’s subordinated debt. |
| Critically undercapitalized          | Same as significantly undercapitalized banks and undercapitalized banks that have failed to submit and implement an acceptable CRP, plus\(^c\)  
• receivership or conservatorship within 90 days (extensions permitted under certain circumstances with OCC approval and FDIC concurrence), or such other action the OCC determines, with the concurrence of the FDIC, will resolve the bank’s problems at the least possible long-term cost to the Deposit Insurance Fund better than receivership or conservatorship.  
• restrictions on payments of principal or interest on the bank’s subordinated debt. |

\(^a\) Refer to 12 USC 1831f, 12 CFR 303.243 and 12 CFR 337.6. Deposit rate restrictions prevent a bank that is not well capitalized from circumventing the prohibition on brokered deposits by offering rates significantly above market in order to attract a large volume of deposits quickly. As a general rule, a bank that is not well capitalized may not offer deposit rates more than 75 basis points above average national rates for deposits of similar size and maturity. Refer to FDIC FIL-42-2016, “Frequently Asked Questions on Identifying, Accepting and Reporting Brokered Deposits,” for more information.

\(^b\) There is the presumption that the OCC will take these actions.

\(^c\) The FDIC shall also prescribe certain further restrictions on the activities of the bank.
Appendix E: Resolution

For purposes of this appendix, the term “bank” refers only to an “insured depository institution” as defined in 12 USC 1813(c)(2).

Pursuant to 12 USC 1831o(h)(3), the OCC is required to place a bank into receivership when the bank is insolvent or has a ratio of tangible equity to total assets that is equal to or less than 2 percent, unless the OCC, with FDIC concurrence, takes other actions the OCC determines would better achieve the purpose of 12 USC 1831o. Once a bank’s ratio of tangible equity to total assets has dropped to 2 percent or below, the bank is subject to all restrictions and limitations applicable to critically undercapitalized banks, including the provisions of 12 USC 1831o(h)(3) pertaining to receivership or conservatorship.

The OCC also has the authority to initiate resolution by placing a bank into receivership or conservatorship or requiring its sale, merger, or liquidation while the bank still has a ratio of tangible equity to total assets of more than 2 percent in certain circumstances. Such action may help resolve a bank at the least long-term cost to the Deposit Insurance Fund by reducing or limiting losses that might otherwise result if the bank were allowed to remain open until its ratio of tangible equity to total assets has dropped to 2 percent or less, or its capital has been exhausted. In certain cases, resolution may be considered if the bank

- is losing capital.
- has no realistic prospects for recapitalization.
- is engaging in practices likely to increase losses in the future.
- is engaging in unsafe or unsound practices that have a substantial negative effect on the bank.
- suffers from other critical management failures identified in the receivership statutes.

When a bank first becomes undercapitalized for PCA purposes, or when a bank that is not yet undercapitalized begins to show substantial safety and soundness weaknesses or other critical management failings, the supervisory office should develop a resolution contingency plan involving a merger, sale, voluntary liquidation, conservatorship, or receivership. Planning for these potential future developments is a factor in selecting which bank enforcement actions to use in the near term.

The supervisory office must take into account the long-range strategy for the bank in deciding which bank enforcement action to use. Using bank enforcement actions at the rehabilitation stage can enhance the OCC’s position for resolution, if the need arises. For example, for an undercapitalized bank, the failure to submit and implement an acceptable CRP is a ground for receivership. It may also be a basis to require the bank to be sold or merged into another bank. Similarly, when addressing substantial safety and soundness weaknesses or other critical management failings, a C&D order might be preferred because a willful violation of a C&D (or consent) order is itself a ground for receivership. In addition, PCA, C&D (or consent) order, and safety and soundness order processes all have provisions authorizing the OCC to require a bank to take any action the OCC determines will best resolve the bank’s deficiencies. In appropriate
cases, this authority could be used to require that the bank have a contingency plan to sell or liquidate itself if it does not remedy its deficiencies within a specified time period.

The supervisory office should consider whether resolution would be appropriate when a bank has reached the point when additional bank enforcement actions will likely not prevent insolvency or reduce the cost to the Deposit Insurance Fund. Once a decision is made to adopt a resolution approach, OCC resources should be focused on the best available option at the least cost to the Deposit Insurance Fund.

The facts and reasons on which the receivership or other resolution is based must be well supported and documented in the OCC’s supervisory information systems. In most instances, prior bank enforcement actions will have addressed these matters at an earlier stage (for example, when the bank first became undercapitalized or when the bank was required to remedy unsafe or unsound practices in an enforcement action). The record prepared for those actions will later be a part of documenting the receivership grounds. Additional documentation of the continuation and worsening of deficiencies or a substantial negative impact on the bank’s assets, earnings, or ability to conduct business is needed to support receivership grounds.
Appendix F: Compliance With Enforcement Actions Page Template

We performed an assessment of the bank’s compliance with each actionable article of the [enforcement action type]. A rating of “in compliance” can be achieved on a particular article in an enforcement action only after the bank has adopted, implemented, and adhered to all of the corrective actions set forth in the article; the corrective actions are effective in addressing the bank’s problems; and OCC examiners have verified and validated through the examination process that these measures have been accomplished and are sustainable.

An assessment of “not in compliance” means either of the following conditions:

- Additional action on the part of the bank, the board, and management is required, such as when the board or management have failed to adopt policies, procedures, or systems within required time frames; when adopted policies, procedures, and systems fail to address all required items in the article; when the bank has failed to comply with immediately effective requirements or has failed to cease activities prohibited by the article; or when the board or management has failed to fully implement or adhere to corrective actions.

- The bank has adopted and begun the implementation of all of the corrective actions required by the article, but sufficient time has not passed to validate that the actions have been fully implemented, are being adhered to, and are effective and sustainable in addressing the bank’s problems. In these situations, the board and management must continue to monitor and test the bank’s progress to ensure corrective actions are fully implemented, adhered to, and effective.

If the action is a capital directive, C&D order, consent order, GLBA agreement, formal agreement, PCA directive, safety and soundness order, operating agreement, or conditions imposed in writing, use this paragraph: The board is reminded that failure to comply with the [type of enforcement action] is an unsafe or unsound banking practice, except when noncompliance is due solely to the need for additional time to assess the effectiveness of corrective actions. Continued noncompliance with the [type of enforcement action] will delay restoring the bank to a satisfactory condition. Failure to fully address and adhere to the [type of enforcement action] may result in more severe enforcement actions, including potential civil money penalties (CMPs) against the bank, individual members of the board, or management.

If the action is a commitment letter, IMCR, MOU, or 12 CFR 30 notice of deficiency, use this paragraph: The board is reminded that failure to comply with the [type of enforcement action] may be an unsafe or unsound banking practice, except when noncompliance is due solely to the need for additional time to assess the effectiveness of corrective actions. Failure to fully address and adhere to the [type of enforcement action] may result in more severe enforcement actions against the bank, individual members of the board, or management.

The bank remains not in compliance with [number] of the [number] actionable articles in the [type of enforcement action]. The following descriptions of the articles are abbreviated. The board and management must not rely on these condensed descriptions and should refer to the [type of enforcement action] itself for specific requirements. The board is cautioned that
continued diligence in complying with all articles is required, as “in compliance” designations are subject to regular reevaluation until such time that the enforcement action is terminated.

We have included management’s revised commitments to address the remaining corrective action requirements. Nothing in this [report or letter] should be interpreted to suggest that we are granting any extensions or find the bank’s commitments as satisfactory or sufficient to meet the requirements of the respective articles. The following is a summary of the bank’s progress in addressing the requirements of each actionable article.

<table>
<thead>
<tr>
<th>Article #</th>
<th>Title of Article</th>
<th>Status</th>
</tr>
</thead>
</table>

[Insert a brief summary of the article’s requirements.]

**Status:** Discuss the status of the article.

- Include specific facts to support “compliance” or “not in compliance” determination.
- If the article is not in compliance but is also “past due” or “pending validation,” state that here.
- If the article is in compliance, this section should state that compliance with the article will continue to be assessed until the enforcement document is terminated.

**Additional Action Required**

- State what the bank must do to achieve compliance with the article.
- Requirements must be specific, actionable, and consistent with the article.

**Commitment**

Discuss the management’s or the board’s commitments to the additional actions required.

- Be as specific as possible.
- Include dates and the names of persons responsible.

Omit this section if the article is in compliance.
Appendix G: Sample Write-Ups for Compliance With Enforcement Actions Section of a Formal Written Communication

This appendix includes sample write-ups for the “Compliance With Enforcement Actions” section of a formal written communication. This section of a formal written communication should include the standard text in appendix F followed by a table summarizing the status of each article. In the formal communication, the write-ups should be listed after the table.

Example 1: Article Not in Compliance, Past Due

**Article II—Strategic Plan—Not in Compliance (Past Due)**

*This article requires the board to submit a strategic plan covering at least a three-year period. The article requires the board to prepare and submit a quarterly written evaluation of the bank’s performance against the plan once it receives a written determination of no supervisory objection for the plan. Until the strategic plan receives a determination of no supervisory objection, the bank shall not significantly deviate from the operations that existed prior to the order without first receiving the OCC’s prior written determination of no supervisory objection.*

**Status:** Corrective actions required by this article are past due. The board submitted a strategic plan to the OCC on September 15, 20XX, but the strategic plan fails to address all items required by the order. Specifically, the strategic plan does not include personnel responsible for achieving various goals and initiatives, a clear description of control systems to mitigate risks associated with new products, growth, or changes in bank markets, and a description of systems designed to monitor the bank’s progress. The strategic plan also includes significant loan growth in new loan products without appropriate policies and risk management systems.

**Additional action required:** The board has a continuing obligation to submit an acceptable strategic plan covering at least a three-year period that addresses all requirements of this article. Upon approval by the board, the three-year strategic plan must be submitted to the OCC for review, and a determination of no supervisory objection must be made prior to implementation.

**Commitment:** CEO Johnson committed to revising the strategic plan to address all requirements of the order by January 31, 20XX.

Example 2: Article Not in Compliance, Pending Validation

**Article III—Internal Audit Program—Not in Compliance (Pending Validation)**

*This article requires the board or audit committee to develop and adhere to a satisfactory, independent internal audit program. The board or audit committee shall ensure timely follow-up and correction of deficiencies identified by internal audit.*

**Status:** The audit committee has developed a satisfactory audit program. Jane Doe was hired as the bank’s chief audit executive on October 1, 20XX. The audit department is appropriately
staffed. Additionally, the risk assessment and schedule have been improved to include all relevant areas. Additional time needs to pass, however, for auditor Doe and the audit committee to demonstrate the adequacy and sustainability of the program.

**Additional action required:** The audit committee must ensure implementation of the audit program and ensure timely follow-up and correction of deficiencies by internal audit.

**Commitment:** Audit committee chairman Smith committed to ensuring implementation of the audit program and correction of deficiencies identified by internal audit.

**Example 3: Article in Compliance**

**Article IV—Allowance for Loan and Lease Losses—Compliance**

This article requires the board to revise the bank’s program for the maintenance of an adequate allowance for loan and lease losses (ALLL). The bank’s ALLL policy and methodology must be consistent with GAAP; OCC Bulletin 2006-47, “Interagency Policy Statement on the Allowance for Loan and Lease Losses”; the “Allowance for Loan and Lease Losses” booklet of the Comptroller’s Handbook; and the call report instructions.

**Status:** The board approved a revised ALLL policy on September 15, 20XX, that addresses requirements of the article. Examiners validated the effectiveness of the revised ALLL policy and determined that the revised methodology is appropriate and is consistent with GAAP; OCC Bulletin 2006-47; the “Allowance for Loan and Lease Losses” booklet of the Comptroller’s Handbook; and the call report instructions. The methodology has been in place for four consecutive quarters and was also validated by the bank’s internal audit.
# Appendix H: Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>anti-money laundering</td>
</tr>
<tr>
<td>BSA</td>
<td>Bank Secrecy Act</td>
</tr>
<tr>
<td>CAMELS</td>
<td>rating system with six component areas: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk</td>
</tr>
<tr>
<td>C&amp;D</td>
<td>cease-and-desist</td>
</tr>
<tr>
<td>CFR</td>
<td>U.S. Code of Federal Regulations</td>
</tr>
<tr>
<td>CMP</td>
<td>civil money penalty</td>
</tr>
<tr>
<td>DSRC</td>
<td>District Supervision Review Committee</td>
</tr>
<tr>
<td>FDIC</td>
<td>Federal Deposit Insurance Corporation</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm–Leach–Bliley Act</td>
</tr>
<tr>
<td>IMCR</td>
<td>individual minimum capital ratios</td>
</tr>
<tr>
<td>ITCC</td>
<td>information technology, trust, consumer compliance, and Community Reinvestment Act</td>
</tr>
<tr>
<td>MMSRC</td>
<td>Major Matters Supervision Review Committee</td>
</tr>
<tr>
<td>MOU</td>
<td>memorandum of understanding</td>
</tr>
<tr>
<td>MRA</td>
<td>matter requiring attention</td>
</tr>
<tr>
<td>MSRC</td>
<td>Midsize Supervision Review Committee</td>
</tr>
<tr>
<td>OCC</td>
<td>Office of the Comptroller of the Currency</td>
</tr>
<tr>
<td>OOI</td>
<td>order of investigation</td>
</tr>
<tr>
<td>PCA</td>
<td>prompt corrective action</td>
</tr>
<tr>
<td>PPM</td>
<td>Policies and Procedures Manual</td>
</tr>
<tr>
<td>ROCA</td>
<td>risk management, operational controls, compliance, asset quality</td>
</tr>
<tr>
<td>ROE</td>
<td>report of examination</td>
</tr>
<tr>
<td>SRC</td>
<td>supervision review committee</td>
</tr>
<tr>
<td>USC</td>
<td>U.S. Code</td>
</tr>
<tr>
<td>WSRC</td>
<td>Washington Supervision Review Committee</td>
</tr>
</tbody>
</table>
Appendix I: References

References are generally applicable to national banks and federal savings associations unless otherwise noted.

Laws

12 USC 24a(e)(2) and (3), “Provisions Applicable to National Banks That Fail to Continue to Meet Certain Requirements”
12 USC 1464, “Federal Savings Associations” (federal savings associations)
12 USC 1813(c)(2), “Definitions Relating to Depository Institutions”
12 USC 1818, “Termination of Status as Insured Depository Institution”
12 USC 1818(b), “Cease-and-Desist Proceedings”
12 USC 1818(c), “Temporary Cease-and-Desist Orders”
12 USC 1818(i), “Jurisdiction and Enforcement; Penalty”
12 USC 1818(s), “Compliance With Monetary Transaction Recordkeeping and Reporting Requirements”
12 USC 1818(u), “Public Disclosures of Final Orders and Agreements”
12 USC 1821(c)(5), “Insurance Funds, Appointment of Corporation as Conservator or Receiver”
12 USC 1831f, “Brokered Deposits”
12 USC 1831a, “Prompt Corrective Action”
12 USC 1831p-1, “Standards for Safety and Soundness”
12 USC 3102, “Establishment of Federal Branches and Agencies by Foreign Bank” (federal branches and agencies)
12 USC 3108, “Regulation and Enforcement” (federal branches and agencies)
12 USC 3110, “Penalties” (federal branches and agencies)
12 USC 3907, “Capital Adequacy”
12 USC 3909(d), “Civil Penalties; Assessment and Collection”

Regulations

12 CFR 3, “Capital Adequacy Standards”
12 CFR 4, subpart C, “Release of Non-Public OCC Information”
12 CFR 5, “Rules, Policies, and Procedures for Corporate Activities”
12 CFR 5.51, “Changes in Directors and Senior Executive Officers of a National Bank or Federal Savings Association”
12 CFR 6, “Prompt Corrective Action” (national banks and federal savings associations)
12 CFR 28.19, “Enforcement” (federal branches and agencies)
12 CFR 30, “Safety and Soundness Standards”
12 CFR 165, “Prompt Corrective Action” (federal savings associations)
12 CFR 303.243, “Brokered Deposit Waivers”
12 CFR 337.6, “Brokered Deposits”
12 CFR 359, “Golden Parachute and Indemnification Payments”
Policies and Procedures Manual

PPM 5000-7, “Civil Money Penalties”
PPM 5310-5, “Securities Activities Enforcement Policy”
PPM 5310-8, “Fast Track Enforcement Program”
PPM 5310-13, “Institution-Affiliated Party Enforcement Actions and Related Matters”

Other Publications

“Changes in Directors and Senior Executive Officers,” Comptroller’s Licensing Manual
OCC Bulletin 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”
OCC Bulletin 2018-33, “Prompt Corrective Action: Guidelines and Rescissions”