FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2019-05: COMPLIANCE RISK MANAGEMENT

Purpose

This advisory bulletin (AB) communicates to Fannie Mae and Freddie Mac (the Enterprises) the Federal Housing Finance Agency's (FHFA) supervisory expectations for a compliance risk management program (compliance program)[1] to maintain the safety and soundness of the Enterprises' operations. The sophistication of the compliance program should be proportionate to each Enterprise's size, complexity, and risk profile. The compliance program should be designed to promote compliance with applicable laws, regulations, rules, prescribed practices, internal policies and procedures, and ethical and conflict-of-interest standards (compliance obligations).

Background

Compliance risk is the risk of legal or regulatory sanctions, damage to the current or projected financial condition, damage to business resilience, or damage to reputation resulting from nonconformance with compliance obligations.[2] In addition, an Enterprise may be exposed to compliance, reputational, or other risks as a result of a third-party provider's failure to comply with the Enterprise's expectations and operating standards and to meet all relevant legal and contractual requirements. An effective compliance program supports safe and sound operations

[1] 12 CFR 1239.12.

[2] The regulation requires that the compliance program manage compliance with "applicable laws, rules, regulations, and internal controls," 12 CFR 1239.12.

through policies and procedures designed to enable oversight of compliance risk management by the board of directors, or appropriate board-level committee (board).

Effective management of compliance risk requires the Enterprises to address numerous complex compliance obligations and the Enterprises' high volume of transactions. The guiding principles of sound risk management are set forth in FHFA's regulation at 12 CFR Part 1239, Responsibilities of Boards of Directors, Corporate Practices and Corporate Governance (Corporate Governance Rule), and in the Appendix to 12 CFR Part 1236, Prudential Management and Operations Standards (PMOS).

FHFA's general standards for safe and sound operations are set forth in the PMOS. Three relevant PMOS articulate guidelines for an Enterprise's board of directors and senior management to evaluate when establishing internal controls and information systems (Standard 1), overall risk management processes (Standard 8), and maintenance of adequate records (Standard 10). While the guiding principles of sound risk management in the Corporate Governance Rule and the PMOS are the same for compliance risk as for other types of risk, the management of compliance risk presents certain unique challenges. For example, compliance risk appetite and metrics may be difficult to establish and measure and compliance obligations must be addressed on an Enterprise-wide basis.[3] In addition, while compliance risks associated with third-party providers may be difficult to monitor based on information gathered in the normal course of business, the Enterprises should anticipate and manage exposures associated with third-party provider relationships across the Enterprises' full range of operations.[4]

Guidance

FHFA expects each Enterprise to have a comprehensive, risk-based compliance program aligned with its enterprise-wide risk management program[5] and in accordance with all relevant FHFA guidance. An Enterprise's compliance program should include policies and procedures designed to manage compliance risk across its entire organization, both within and across business lines and the three lines of defense. The compliance program should include the following components:

1) Compliance Governance
2) Compliance Policies and Procedures

---

[3] 12 CFR 1239.11(b), 1239.11(b)(2)(i), and 1239.11(c)(2).

[4] See *Oversight of Third-Party Provider Relationships*, AB 2018-08. See also PMOS, Standard 9: Principles 4, 5, and 10.

[5] 12 CFR 1239.11(a).

3) Compliance Staffing and Compensation
4) Compliance Monitoring, Testing, and Remediation
5) Compliance Communication and Training

1) Compliance Governance

The board should have an appropriate understanding of the types of compliance risks to which the Enterprise is exposed.[6] The board is responsible for exercising reasonable oversight to ensure that the compliance program is designed, implemented, reviewed, and revised in an effective manner.[7] The compliance program must be headed by a compliance officer[8] with the appropriate qualifications, experience, authority, accountability, and independence.[9] It should also be aligned with the enterprise-wide risk management program and board-approved risk appetites, including limits restricting exposures to third-party providers.[10] The board and senior management[11] should ensure that the compliance officer and the compliance program have adequate resources, including well-trained and capable staff.[12]

The board and senior management must discharge their duties and responsibilities in accordance with the Enterprise's code of conduct and ethics, and conduct themselves in a manner that promotes high ethical standards and a culture of compliance throughout the organization.[13] Promoting a culture of compliance includes documenting and communicating clear expectations about compliance both within the Enterprise and to third-party providers including sellers and servicers. The following activities are also part of an effective compliance culture: clearly communicating the Enterprise's compliance, integrity, and business ethics standards and expectations; articulating the principle that employees and management conduct all activities in accordance with both the letter and the spirit of compliance obligations; and creating an

---

[6] See generally PMOS, *Responsibilities of the Board of Directors:* Principle 4.
[7] Ibid.
[8] 12 CFR 1239.12.
[9] PMOS, Standard 1: Principle 2 and Standard 8: Principles 1 and 3.
[10] See *Oversight of Third-Party Provider Relationships,* AB 2018-08.
[11] Ibid. The term "senior management" refers to those employees who plan, direct, and formulate policies, and provide the overall direction of the Enterprise for the development and delivery of products or services, within the parameters approved by the board.
[12] PMOS, *General Responsibilities of the Board of Directors and Senior Management*: Principle 6 and Standard 8: Principle 6.
[13] 12 CFR 1239.10(a). See also PMOS, Standard 1: Principle 3.

environment where employees are encouraged to raise legal, compliance, and ethics questions and concerns without fear of retaliation.

The compliance officer must report directly to the chief executive officer[14] and should have sufficient resources and qualified staff to implement the compliance program. The compliance officer must also report regularly to the board.[15] At a minimum, these reports must address the adequacy of the Enterprise's compliance policies and procedures, including the entity's compliance with them. The compliance officer must recommend any revisions to such policies and procedures that he or she considers necessary or appropriate.[16]

First-line business functions own and manage compliance risks and implement corrective actions to address process and control deficiencies. The second line performs various risk control and compliance oversight functions. The scope and breadth of the activities of the compliance program should be subject to periodic review by the internal audit function.[17] The internal audit function's assessment of the effectiveness of the compliance program should be separate from the compliance function's monitoring and testing activities to ensure that the activities of the compliance function are subject to independent review.[18]

2) Compliance Policies and Procedures

The processes and systems for managing compliance risk across the Enterprise should be documented in policies and procedures. The policies and procedures should also address compliance training throughout the organization.

Compliance policies should clearly articulate the roles and responsibilities of the various committees, functions, and staff with compliance responsibilities as well as the oversight role and responsibilities of the compliance officer and the board. These policies should describe the responsibilities of the compliance officer for managing and directing the implementation of the compliance program and the compliance officer's role in controlling compliance risks that transcend business lines. The policies should also address the scope of internal reporting of

[14] 12 CFR 1239.12.
[15] Ibid.
[16] Ibid.
[17] See *Internal Audit Governance and Function,* AB 2016-05. See also PMOS, Standard 1: Principle 14.
[18] See generally PMOS, Standard 2.

compliance matters to the board and senior management and the adequacy of the Enterprise's compliance policies and procedures, including the Enterprise's compliance with them.[19]

The Enterprises should have policies and procedures in place to create an inventory of compliance obligations, identify new and revised compliance obligations, evaluate the impact to the business units, map obligations to internal controls, communicate changes with impacted parties and business units, promote independent reviews and escalation as necessary, and address compliance obligations in a practical and efficient way.

Each Enterprise's compliance program should include compliance risk and control assessment policies and procedures designed to evaluate compliance risks associated with the Enterprise's business activities, including the development of new products and business practices. The compliance program's compliance risk assessment policies and procedures should include methods of measuring compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessments.

Each Enterprise should have policies and procedures to file with FHFA any reports that may be required.[20] These external reporting compliance policies and procedures should address conditions imposed in writing or written agreements between FHFA and the Enterprise.[21]

The Enterprises should have first-line policies and procedures that are designed to implement enterprise-wide compliance policies and to integrate or "operationalize" compliance obligations into day-to-day business processes, job duties, and responsibilities. First-line compliance policies and procedures should also promote independent reviews, identification of compliance issues, and escalation and tracking of identified issues.

Procedures should describe the second-line compliance function's role in determining how business line compliance matters are addressed. Procedures for resolving disputes between the corporate compliance function and business line management regarding compliance matters should ensure that such disputes are resolved objectively. Under such procedures, the final decision-making authority should rest either with the corporate compliance function, or with a committee of senior management, including the compliance officer, that has no business line responsibilities.

---

[19] 12 CFR 1239.12.
[20] 12 CFR 1239.13.
[21] Ibid.

3) Compliance Staffing and Compensation

The compliance officer should have appropriate qualifications, experience, authority, accountability, and independence. The compliance officer should have the necessary resources to implement the compliance function effectively. The compliance officer's compensation should include incentives tied to actions and outcomes within his or her control and influence and not include incentives that could impair or appear to impair the compliance program's independence. The compensation should also comply with 12 CFR Part 1230[22] as well as conform to the Enterprise's policies on compensation and performance management.

The Enterprise should have a sufficient number of staff assigned to the compliance function with requisite knowledge of business activities and compliance obligations to assess compliance risk and the effectiveness of risk controls. The compliance function may be centrally organized with dedicated staff or structured as a hybrid with first-line staff having both business and compliance responsibilities. In a hybrid approach, responsibilities for compliance activities may be delegated within the Enterprise, but oversight and ultimate responsibility for fostering an enterprise-wide compliance approach are borne centrally by the corporate compliance function. If a hybrid structure is used, compliance staff in the first line should have the ability and willingness to effectively challenge business operations regarding risk arising from the Enterprise's activities. The Enterprise should implement appropriate controls and enhanced second-line oversight to identify and address issues that may arise from conflicts of interest affecting compliance staff within the business lines. For example, in these circumstances, the Enterprise should adopt enhanced processes for the second-line compliance function's oversight of monitoring and testing activities performed by compliance staff within the business lines. In a hybrid structure, the second-line compliance function should also play a role in personnel actions and compensation decisions affecting first-line staff with compliance responsibilities. Compensation and incentive programs should avoid undermining the independence and objectivity of first-line compliance activity.

4) Compliance Monitoring, Testing, and Remediation

Compliance monitoring, testing, and remediation efforts should be risk-based, reflect the results of compliance risk assessments, and evaluate the adequacy and effectiveness of compliance activities across the organization. Testing and monitoring activities should provide information to compliance staff and senior executives about the operation of compliance controls across the

[22] As senior vice presidents, the Enterprises' compliance officers fit within the regulatory definition of executive officer. See 12 CFR 1230.2.

organization, provide evidence to support an assessment of the operating effectiveness of the compliance program, and identify actual and potential instances of noncompliance.

Monitoring activities should identify control weaknesses that may fail to prevent or fail to identify noncompliance and should be designed to identify potential issues before a problem develops into noncompliance. These activities may include pre-activity approvals, transaction reviews, in-process quality checks, and outcome data reviews. The Enterprises' compliance programs should also include monitoring of third-party provider relationships to assess compliance with consumer protection-related laws and regulations and oversight of third-party providers' consumer compliance-related policies, procedures, internal controls, and training.[23]

Testing should assess the reliability of key assumptions, data sources, and procedures used in measuring and monitoring compliance risk. Controls should be tested on a periodic basis to ensure they are working as intended. If compliance controls are embedded in automated tools or business unit procedures, qualified compliance staff should review these tools and processes for consistency with entity-wide compliance policies and procedures.

The results of monitoring and testing activities should drive timely remediation of identified weaknesses. Corrective actions should be tracked and escalated as appropriate. Monitoring and testing protocols should include procedures for remedying undue delay in management response or ineffectual remediation efforts.

5) Compliance Communication and Training

The Enterprises should have lines of communication for employees to seek guidance and report concerns about compliance obligations. All Enterprise staff should receive specific, comprehensive compliance training appropriate to each individual's job responsibilities. Training should reinforce the Enterprise's written compliance risk management policies and procedures. When compliance policies are adopted or changed, the Enterprise should assess what, if any, training is appropriate. The Enterprise should determine whether the training should be conducted on an entity-wide or business unit level, who should be trained, and when the training should occur.

[23] PMOS, Standard 9: Principles 4, 5, and 10. See also *Oversight of Third-Party Provider Relationships*, AB 2018-08.

Related Guidance and Regulations

12 CFR Part 1230, Executive Compensation.

12 CFR Part 1236, Appendix, Prudential Management and Operations Standards.

12 CFR Part 1239, Responsibilities of Boards of Directors, Corporate Practices, and Corporate Governance.

Oversight of Third-Party Provider Relationships, Federal Housing Finance Agency Advisory Bulletin 2018-08, September 28, 2018.

Oversight of Multifamily Seller/Servicer Relationships, Federal Housing Finance Agency Advisory Bulletin 2018-05, August 14, 2018.

Internal Audit Governance and Function, Federal Housing Finance Agency Advisory Bulletin 2016–05, October 7, 2016.

Fraud Risk Management, Federal Housing Finance Agency Advisory Bulletin 2015-07, September 29, 2015.

Oversight of Single-Family Seller/Servicer Relationships, Federal Housing Finance Agency Advisory Bulletin 2014-07, December 1, 2014.

Operational Risk Management, Federal Housing Finance Agency Advisory Bulletin 2014-02, February 18, 2014.

Contingency Planning for High-Risk or High-Volume Counterparties, Federal Housing Finance Agency Advisory Bulletin 2013-01, April 1, 2013.

FHFA has statutory responsibility to ensure the safe and sound operations of the regulated entities and the Office of Finance. Advisory bulletins describe FHFA supervisory expectations for safe and sound operations in particular areas and are used in FHFA examinations of the regulated entities and the Office of Finance. Questions about this advisory bulletin should be directed to: SupervisionPolicy@fhfa.gov.