FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2020-06: Enterprise Risk Management Program

Purpose

This advisory bulletin (AB) provides Federal Housing Finance Agency (FHFA) guidance for an effective enterprise risk management (ERM) program to maintain safe and sound operations at Fannie Mae and Freddie Mac (the Enterprises).[1] The ERM program establishes the foundation and sets the framework for an Enterprise's enterprise-wide risk management practices and processes. Therefore, this AB applies to all risk management activities undertaken by the Enterprises and is consistent with risk area-specific guidance. The sophistication of the ERM program should be commensurate with the Enterprise's capital structure, risk appetite, size, complexity, activities, and other appropriate risk-related factors.

Background

Minimum regulatory standards relating to the responsibilities of each Enterprise's board of directors (board), corporate practices, and corporate governance are prescribed in FHFA's regulation, Responsibilities of Boards of Directors, Corporate Practices, and Corporate Governance Matters (Corporate Governance Rule), 12 CFR Part 1239. The Corporate Governance Rule prescribes requirements for an Enterprise to adopt and establish an ERM program that incorporates the Enterprise's risk appetite, aligns the risk appetite with the Enterprise's strategies and objectives, addresses the Enterprise's material risk exposures, and complies with all applicable FHFA regulations and policies. FHFA's Prudential Management and Operations Standards (PMOS), Appendix to 12 CFR Part 1236, set forth the general responsibilities of the board and senior management, as well as specific responsibilities for management and operations relating to ten enumerated standards, adopted as guidelines. Standard 1 (Internal Controls and Information Systems) and Standard 8 (Overall Risk Management Processes) highlight the need for the Enterprises to establish risk management practices that identify, assess, control, monitor, and report enterprise-wide risk exposures and the need to have appropriate risk management policies, standards, procedures, controls, and reporting systems.

[1] Common Securitization Solutions, LLC (CSS) is an "affiliate" of both Fannie Mae and Freddie Mac, as defined in the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended. 12 USC 4502(1).

This AB articulates FHFA's supervisory expectations that the Enterprises' ERM programs and processes are designed to be consistent with safety and soundness standards and applicable laws and regulations. FHFA is issuing this AB to provide an additional level of detail regarding ERM governance and organizational structure, risk appetite and limit-setting, and risk identification, assessment, control, monitoring, and reporting processes. This guidance reflects FHFA's supervisory expectations for the Enterprises to develop a holistic, enterprise-wide view of the most significant risks to the achievement of strategic and business objectives and a framework for effectively managing risk within bounds of risk appetite and tolerance. An effective ERM program considers the overlap and interrelationship of risks; however, that does not relieve an Enterprise from its obligation to identify and manage all on- and off-balance sheet risks that may be more localized or contained within specific portfolios and business line-levels. Additionally, this guidance is informed by FHFA's understanding of current industry standards and enterprise-wide risk management best practices at large, complex financial institutions, incorporating principles and concepts from the Committee of Sponsoring Organizations of the Treadway Commission (COSO),[2] the Financial Stability Board,[3] and enterprise-wide risk management guidance issued by the federal banking regulators.[4]

Guidance

The Enterprises are required to establish and maintain a comprehensive ERM program in accordance with all applicable laws and regulations. Pursuant to the Corporate Governance Rule, an Enterprise must establish and maintain a comprehensive ERM program that establishes the Enterprise's risk appetite and aligns the risk appetite with the Enterprise's strategies and objectives.[5] The ERM program must include business line-appropriate risk limits consistent with risk appetite and provisions for monitoring compliance with the risk limit structure.[6] The ERM program must also have appropriate corporate risk policies and procedures relating to risk management governance, risk oversight infrastructure, processes and systems for identifying and reporting risks, including emerging risks, and timely implementation of corrective actions.[7] Corporate risk policies should be supported, as applicable, by appropriate standards defining minimum requirements. Additionally, the ERM program must include provisions specifying ERM

[2] *See* Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrating with Strategy and Performance* (2017).
[3] See, e.g., Financial Stability Board, *Principles for an Effective Risk Appetite Framework* (2013).
[4] See, e.g., Office of the Comptroller of the Currency, *Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations* (12 CFR Parts 30, 168, and 170) (2014).
[5] 12 CFR 1239.11(a).
[6] 12 CFR 1239.11(a)(3).
[7] 12 CFR 1239.11(a)(3).

management's authority and independence to carry out risk management responsibilities and the integration of risk management with Enterprise management's goals and compensation structure.[8]

An Enterprise's ERM program should have interrelated components that work together to ensure comprehensive and integrated enterprise-wide risk management practices and oversight approaches that are the basis for managing risk in a consistent manner. The ERM program should include the following components:

I. ERM Governance and Organizational Structure
II. Risk Appetite Framework
III. ERM Identification, Assessment, Control, and Monitoring Processes
IV. ERM Reporting and Communication Processes

I. ERM Governance and Organizational Structure

A. Governance Structure

The board must establish a board-level risk committee to assist in carrying out its responsibility for enterprise-wide risk management oversight.[9] The board risk committee must periodically review and recommend to the full board for approval an appropriate ERM program commensurate with the Enterprise's capital structure, risk appetite, complexity, activities, size, and other appropriate risk-related factors.[10] An enterprise risk committee (ERC) should be established as the central management-level risk oversight committee, chaired by the enterprise-wide Chief Risk Officer (CRO), with membership across business functions and risk areas in order to drive a consistent approach to risk oversight. ERC responsibilities should include monitoring and overseeing risk across the Enterprise, which includes reviewing, and, as applicable, approving corporate risk policies and supporting standards; reviewing risk appetite and limits for approval by the board; monitoring key risk indicators; and reviewing risk reports and issues escalated by subordinate management-level risk committees. An Enterprise may establish other management-level committees aligned to specific risk and business-line areas to facilitate enterprise-wide risk oversight duties. Additional first-line risk committees may also be established to facilitate discussion, reporting, and escalation. Collectively, these committees support effective risk governance by providing a forum for transparent communication and documentation[11] of risk management and control activities across functional lines. They also provide an organized pathway for risk reporting, escalation, and issue resolution management.

[8] 12 CFR 1239.11(a)(3).
[9] 12 CFR 1239.11(b).
[10] 12 CFR 1239.11(b)(2)(i).
[11] Regarding documentation of board risk committee meetings, see 12 CFR 1239.11(b)(1)(iv). Documentation of management-level meetings may include memorializing committee discussions in committee minutes and meeting materials.

The Enterprise's risk management organizational structure and the assignment of roles and responsibilities should generally comprise a "three lines model" and approach to risk management. The three lines model forms a strong risk management framework and enables effective enterprise-wide risk management practices. The three lines are:[12]

- First-line business units and corporate support functions, which are accountable for identifying, assessing, controlling, monitoring, and reporting on all risks in executing their functions and operating in a sound control environment;
- Second-line risk management, which provides independent risk oversight and effective challenge of the first line business unit and support functions. Second-line risk management includes the ERM function, along with compliance[13] and other risk oversight functions, as deemed applicable, that monitor risk-taking activities and assess risks and issues independent of first line business units and functions, but still under the direction and control of senior management; and
- Third-line internal audit, which provides timely feedback to management and independent assurance to the board audit committee on the effectiveness of the Enterprise's system of internal controls, risk management, and governance.[14] Third-line internal audit maintains objectivity and independence from management.

B. Roles and Responsibilities

The board is ultimately responsible for enterprise-wide risk management oversight.[15] The board is responsible for approving and periodically reviewing the ERM program, and having it in effect at all times.[16] The board's responsibility for reviewing and approving the ERM program includes establishing the Enterprise's risk appetite and overseeing alignment of risk appetite with the Enterprise's strategies and objectives.[17] The board is responsible for approving the Enterprise's risk appetite addressing material risk exposures and risk limits appropriate to each business line of the Enterprise.[18] The board-level risk committee is responsible for reviewing and recommending the ERM program to the board for approval.[19] Management is responsible for providing adequate reporting to permit the board to remain sufficiently informed about the nature and level of the Enterprise's overall risk exposures so that it can understand the possible short- and long-term

[12] Some organizational units or functions within an Enterprise, such as those that provide legal services to the Enterprise, do not generally fall within a three lines model.
[13] *See* FHFA Advisory Bulletin 2019-05, *Compliance Risk Management* (Oct. 3, 2019).
[14] See FHFA Advisory Bulletin 2016-05, *Internal Audit Governance and Function* (Oct. 7, 2016).
[15] 12 CFR 1239.4(c).
[16] 12 CFR 1239.11(a)(1).
[17] 12 CFR 1239.11(a)(2).
[18] The Corporate Governance Rule defines these as being inclusive of credit, market, liquidity, business, and operational risk. 12 CFR 1239.11(a).
[19] 12 CFR 1239.11(b)(2)(i).

effects of those exposures on the financial and operational health of the Enterprise, including the possible consequences to earnings, liquidity, and economic value.[20]

An Enterprise must appoint an enterprise-wide CRO to head the independent ERM function, with responsibilities for implementing and maintaining appropriate enterprise-wide risk management practices for the Enterprise.[21] The ERM function is responsible for: (1) establishing appropriate corporate risk policies and supporting standards related to risk management governance, practices, and controls; (2) developing appropriate enterprise-wide processes and systems for identifying and reporting current and emerging risks; (3) developing the risk appetite framework, including establishing and recommending for board approval risk appetite statements and risk limits; (4) establishing business-line appropriate risk limits in line with risk appetite and monitoring compliance with such limits; (5) monitoring the level and trend of risk exposures, testing controls, verifying measures for risk exposures used by the business; and (6) communicating enterprise-wide risk management issues and emerging risks, and monitoring effective and timely issue resolution. Independence from the risk-taking business units and functional areas is a cornerstone of an effective ERM function. Although staff performing the ERM function should work closely and coordinate with business unit personnel, they should maintain independence by performing the appropriate oversight and assisting business units with risk analyses. ERM staff should have the expertise to critically review and the independence to effectively challenge the Enterprise's business practices and risk-taking activities.

The CRO must report directly to the board risk committee and to the Chief Executive Officer (CEO) on significant risk exposures and related controls, changes to risk appetite, risk management strategies, results of risk management reviews, and emerging risks.[22] The CRO is also responsible for regularly reporting on the Enterprise's compliance with, and adequacy of, its corporate risk management policies, and must recommend any adjustments as necessary and appropriate.[23] The CRO should also report on compliance with, and adequacy of, supporting corporate risk standards. Individual business or functional risk officers may be designated and delegated risk authority of specific risk areas and functions, as appropriate, to facilitate enterprise-wide risk oversight.

First-line business units and corporate support functions are responsible for managing risks that arise in the execution of their functions. This includes responsibility for identifying, assessing, controlling, monitoring, and reporting risks in alignment with the methodologies as established in corporate risk policies and supporting standards. First-line functions should be aware of applicable risk appetite limits, thresholds, and indicators and their responsibilities associated with managing risks within appetite and escalation and corrective action in the event of breach. All divisions,

[20] *See generally*, 12 CFR Part 1236, Appendix (PMOS), Responsibilities of the Board of Directors, Principle 4.
[21] 12 CFR 1239.11(c).
[22] 12 CFR 1239.11(c)(5).
[23] 12 CFR 1239.11(c)(5).

inclusive of second-line and third-line functions, have operating function responsibilities for managing risks that arise in the execution of their activities.

C. Policies, Standards, and Procedures

The ERM program must include appropriate corporate risk policies and procedures related to risk management governance and practices.[24] At a minimum, this should include a board-approved ERM policy that establishes an integrated framework for managing risks enterprise-wide, describes the risk governance and risk oversight structure, and specifies roles and responsibilities. The ERM function should be responsible for developing and overseeing the implementation of the ERM policy and any supporting corporate risk standards describing the minimum criteria for identifying, assessing, controlling, monitoring, and reporting risks, including emerging risks. First-line functions should have procedures that are designed to implement the expectations for effective risk management as described in the ERM policy and applicable supporting standards. The Enterprise should also have a corporate risk taxonomy that defines common risk categories and classifies hierarchies of risks. The Enterprise should also have in place risk type corporate policies, standards, and implementing procedures consistent with its risk taxonomy categorizations. These risk type policies, standards, and procedures should be consistent with the ERM policy and supporting standards, but further define responsibilities and requirements for managing specific risks.

An enterprise-wide policy or supporting standard should also define expectations for developing, measuring, monitoring, communicating, and reporting on risk appetite, clearly defining roles and responsibilities of the board, management, and business units for managing risk within risk appetite and taking action when in breach of limits. While the ERM function is responsible for designing and overseeing the risk appetite framework, input and engagement across the first line business units and corporate functions should occur to develop risk appetite and the supporting metrics and limits that are ultimately reviewed and approved by the board. A comprehensive set of risk metrics, limits, and associated monitoring activities must be in place to confirm that risk exposures remain within established risk limits.[25] Board risk limits should be supported by defined and actionable thresholds, set at a lower level than the limit to support risk monitoring and prompt management action before the limit is breached. The Enterprise should have processes defining escalation protocols and expectations for timely corrective action in the event of breach of thresholds and limits. This includes a mechanism for reporting breaches of risk limits to senior management and the board or board risk committee.[26]

[24] 12 CFR 1239.11(a)(3).
[25] *See* 12 CFR 1239.11(a) and 12 CFR Part 1236, Appendix (PMOS), Standard 8.
[26] *See* 12 CFR 1236, Appendix (PMOS), Standard 8.

The process for policy approval, exception protocols, and delegations of authority should be clear. Corporate risk policies, supporting standards, and implementing procedures should be reviewed, and updated periodically to consider changes in risk practices and regulatory expectations. The ERM function should regularly monitor first-line implementation and adherence to the ERM policy and related corporate risk policies and supporting standards.

D. Risk Culture

The board and senior management should set the "tone at the top" in a manner that fosters an effective risk culture. Risk culture constitutes the shared values, attitudes, competencies, and behaviors that guide risk decision-making and governance practices throughout the Enterprise. Risk culture emphasizes risk awareness and communicates the Enterprise's expectations for risk management and operating within established risk appetite and limits. An effective risk culture (1) promotes high ethical standards,[27] safety and soundness, compliance, and effective risk management; (2) establishes clear responsibility and accountability; (3) emphasizes the importance of internal control; and (4) promotes risk awareness, collaboration, transparency, and proactive discussion at all levels. Enterprise personnel are expected to be individually accountable, risk aware, perform risk management functions associated with their day-to-day business activities, engage in risk discussions, and escalate risk issues.

Employees at all levels should receive regular training on corporate risk policies, supporting standards, and implementing procedures to enable effective understanding and management of risks. Processes should be in place to ensure employees are accountable and aware of their risk management roles and responsibilities. An effective risk culture is evidenced when the Enterprise's overall risk appetite is aligned with its mission and business objectives; risk reporting is timely, accurate, and informative; and risk management is integrated with management's performance goals, objectives, and compensation structure.[28]

The board or board risk committee and senior management should ensure that the CRO and the ERM function have adequate resources, including a well-trained and capable staff. The CRO should have stature and risk management expertise that is commensurate with the Enterprise's capital structure, risk appetite, complexity, activities, size, and other appropriate risk-related factors. The CRO's performance evaluation and compensation should be structured to provide for an objective and independent assessment of the risks taken by the Enterprise.

II. Risk Appetite Framework

[27] An Enterprise must establish and adhere to a written code of conduct and ethics that is reasonably designed to assure that directors, officers, and employees discharge their duties and responsibilities in an objective an impartial manner that promotes honest and ethical conduct, compliance, and accountability. 12 CFR Part 1239.10(a).
[28] *See* 12 CFR Part 1239.11(a)(3) and 12 CFR Part 1236, Appendix (PMOS), Standard 8.

The ERM program sets the foundation for identifying, measuring, monitoring, and reporting on individual and aggregate levels of risks in relation to established risk appetite and risk limits.

A. Risk Appetite's Relationship to Strategy and Objective Setting

Specific requirements for a board-approved strategic business plan are contained in the Corporate Governance Rule, including, among other things, that the strategic business plan must identify current and emerging risks of the Enterprise's significant existing activities or new activities and include discussion of how the Enterprise plans to address such risks while furthering its public purposes and mission in a safe and sound manner.[29] The Corporate Governance Rule also requires that the Enterprise's risk appetite align with its strategies and business objectives[30] and that the ERM program align with its risk appetite.[31] Risk appetite should be linked to business decision-making, and be considered in light of the Enterprise's business model. The CEO or President should be responsible for integrating and aligning the board-approved risk appetite with the Enterprise's strategic business plan. The ERM program should be integrated into the processes for developing and reviewing the Enterprise's strategic business plan to ensure alignment.

B. Risk Appetite Statement and Risk Limits

The Corporate Governance Rule defines risk appetite as the aggregate level and types of risk the board of directors and management are willing to assume to achieve the Enterprise's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements.[32] Risk appetite should be grounded in the concept of risk capacity, or the maximum amount of risk the Enterprise can absorb before breaching capital, liquidity, and other constraints. An Enterprise's risk appetite should be less than its risk capacity, and its risk profile should not exceed risk appetite. Conceptually, these elements work together to provide a basis for communicating the Enterprise's risk profile and ensuring risk exposures are managed within risk appetite.

An Enterprise's risk appetite framework should include a risk appetite statement and related quantitative risk metrics and limits. The risk appetite statement is an articulation of risk appetite in written form. It should be easy to communicate and understand, such that the board and senior management obtain a holistic but concise and easy to absorb view of the Enterprise's aggregate risk position, aggregated within and across each material risk type, and based on forward-looking assumptions. It should also be easy to communicate and cascade down to the first-line risk taking functions such that it is easy to understand and apply in daily operations. The overall risk appetite statement may be designed as a series of qualitative summary statements describing the

[29] 12 CFR Part 1239.14(a)(5).
[30] 12 CFR Part 1239.11(a).
[31] 12 CFR Part 1239.11(a)(2).
[32] 12 CFR Part 1239.2.

Enterprise's aggregate risk appetite by material risk type. The overall statement, and as appropriate summary statements, should articulate clearly the motivations for accepting or avoiding that type of risk and set clear boundaries and expectations to enable risk monitoring and reporting. The statement should provide context by describing the current business activities that give rise to the risk, the desired risk tolerance, and corresponding mitigating controls and processes in place to allow operation within the stated risk appetite. The statement should include a scale identifying the risk appetite level for each material risk type in a clear and succinct manner. For example, each material risk type should be assigned a single-word consistent with the scale that clearly identifies the Enterprise's posture with regard to that risk type.

While the qualitative risk appetite statement expresses a broad view of the risk in written form, the Enterprise should establish a comprehensive set of quantitative risk metrics, limits, thresholds, and indicators that allocate the Enterprise's risk appetite across material risk types, complement the qualitative statement, and set the overall tone for the Enterprise's approach to risk taking. The Enterprise must have board-approved risk limits[33] and they should be set corresponding to a metric or set of metrics designed to measure a specific risk exposure or portfolio. The board risk limit should be supported by defined and actionable thresholds, set at a lower level than the limit to support risk monitoring and prompt management action before the limit is breached. An Enterprise may establish additional cascading, lower-level management limits and notification thresholds, as appropriate, that are designed to prompt management action. Board-level risk limits are not meant to be exceeded, and therefore an Enterprise should establish a framework for triggering escalations when limits are breached, with defined escalation and reporting protocols. All risk limits should be regularly monitored so that risk exposures remain within established thresholds.[34] If a risk type cannot be quantified into limits and thresholds, qualitative measures and early warning indicators should be developed in order to provide an early signal of increasing risk exposures. These early warning indicators, or other key risk indicators, should be tracked to identify changes to the risk profile and emerging risks. Regular reassessment and update of early warning indicators should occur based on changing environmental and operational conditions.

Risk metrics should reflect attributes of the risk exposure being measured, and be consistent with applicable capital, liquidity, and other regulatory requirements. The limits corresponding to the metric should be set at a level to govern risk-taking within the defined risk appetite. Risk limits should be specific, measurable, actionable, sensitive to portfolio composition, reportable, and based on forward-looking assumptions. Risk limits should be expressed relative to earnings, capital, liquidity, or other relevant measures as appropriate.[35] In setting risk limits, the Enterprise should consider the interaction between risks within and across business lines, and their correlated or compounding impact on exposures and outcomes. As appropriate, the Enterprise should utilize

[33] 12 CFR Part 1239.11(a)(3)(i). See also 12 CFR Part 1236, Appendix (PMOS), Standard 8.
[34] *See* 12 CFR Part 1239.11(a)(3) and 12 CFR Part 1236, Appendix (PMOS), Standard 8.
[35] The PMOS lays out expectations regarding specific risk area risk limit-setting, measurement, and escalation.

scenario analysis and stress testing results to inform the risk appetite limit setting process in order to ensure that the Enterprise understands what events might push it outside its risk appetite or capacity. Risk limits may require model output to measure and monitor exposures and on-top adjustment subject to model risk management and review as appropriate.[36]

The Enterprise's risk appetite framework should be re-evaluated on at least an annual basis to ensure it is representative of any changes in risk profile of the Enterprise and continued alignment to strategic and business objectives. The review should consider significant market and business changes, new business initiatives, risk event occurrences, and other changes to the Enterprise's risk profile. Additional ad hoc reviews should occur periodically during the year considering any major changes outside of the ordinary annual cycle.

III. ERM Identification, Assessment, Control, and Monitoring Processes

The ERM program supports the management of risk exposures through enterprise-wide risk management processes designed to identify, assess, control, monitor, and report risk.

The Enterprise should have processes in place to identify current, new, top, emerging, and changing risks and methods for evaluating the level of exposure to risk. Risks should be rated based upon measures of the likelihood of a risk's occurrence and the severity of its impact. Forward-looking assessments and scenarios should also be used to identify risks that could pose the most significant impacts to the Enterprise, both during periods of normal economic conditions and periods of stress. Risk identification and assessment processes should occur regularly and include comprehensive self-assessment of material risks on at least an annual basis.[37]

The risk assessment process should start with a rating of inherent risk, which represents the level of exposure to a risk absent any management actions to alter the risk's likelihood or impact. The design and operating effectiveness of controls in place to mitigate the risk should then be evaluated. A residual risk rating should result, considering the likelihood and impact of the risk's occurrence taking into account the application and effectiveness of these mitigating controls. An additional risk response is then determined considering the residual risk and applicable risk appetite. Risk responses should result in either accepting, reducing, transferring, pursuing, or avoiding the risk. Risk acceptance results in no action taken to affect the residual risk. Risk reduction results in designing and implementing processes to effectively apply additional mitigating controls to reduce residual risk to an acceptable level. Risk transference results in sharing or transferring a portion of the risk to reduce residual risk to an acceptable level. Risk pursuance results in action taken that accepts increased risk in order to achieve increased performance. Risk avoidance results in discontinuing the activities which give rise to the risk all together. Management's response

[36] *See* FHFA Advisory Bulletin 2013-07, *Model Risk Management Guidance* (Nov. 20, 2013).
[37] 12 CFR Part 1236, Appendix (PMOS), Standard 8.

decision should be informed by risk appetite and other criteria for determining the acceptability of residual risk to the Enterprise.

Risks should be regularly monitored to determine the current status and identify changes or trends in risk exposures over time. First line functions are responsible for establishing monitoring processes on risks arising from the activities for which they are accountable and managing those risks within the established risk appetite. The second line ERM function is responsible for overseeing first line risk monitoring activities and monitoring adherence to risk appetite. Regular monitoring for adherence to the risk appetite and limit structure is necessary to ensure risk exposures remain within established risk limits.[38] The overall effectiveness of the Enterprise's internal control system should be monitored on an ongoing basis and ensure that business units conduct periodic evaluations. Internal control deficiencies should be reported to senior management and the board on a timely basis and addressed promptly.[39]

The Enterprise should have processes in place to identify and define issues that may arise due to internal control gaps or weaknesses or internal process deficiencies. Issues may be identified through regular risk assessment and monitoring processes, second line oversight activities, internal audit reviews, or FHFA examinations, or management self-identified through the normal course of business. Issues should be documented, rated to assess priority, assigned ownership, and addressed in a timely manner. Issue remediation should be regularly monitored and reported to senior management and the board or appropriate board committee.

IV. ERM Reporting and Communication Processes

Information generated from risk management processes should be reported in a form that is relevant, accurate, complete, timely, consistent, and comprehensive to enable the execution of sound and informed risk management decisions.[40] The Enterprise should have risk management information systems that generate, at an appropriate frequency, the information needed to manage risk. Risk data should be aggregated to develop a comprehensive and accurate view of the Enterprise's aggregate risk position and to facilitate integrated enterprise-wide risk reporting. Systems and processes supporting risk and control reporting should align under a common data architecture to facilitate and support the Enterprise's risk aggregation and enterprise-wide reporting. Standardized data that is consistently defined is key when producing enterprise-wide reports that aggregate or combine risk data from different risk management processes. Consistent and standardized risk data is also important for preparing reports that compare risks over time for meaningful trend analysis. Risk reports should be defined to ensure that the reports produced are comprehensive, at an appropriate level, and consistent across board, senior management, and

[38] 12 CFR Part 1236, Appendix (PMOS), Standard 8.
[39] 12 CFR Part 1236, Appendix (PMOS), Standard 1.
[40] *See* FHFA Advisory Bulletin 2016-04, *Data Management and Usage* (Sept. 29, 2016).

business-line levels. Risks identified at process- and business-line levels should be consistent with and flow up to a portfolio and aggregated enterprise-wide view of risk.

The ERM function is responsible for providing a comprehensive enterprise-wide view of risk to the board risk committee and appropriate levels of management for consideration and action. The CRO must report to the board risk committee and to the CEO on significant risk exposures and related controls, adherence to risk appetite and limits, risk management strategies, results of risk management reviews, and emerging risks.[41] The CRO must also report any significant issues related to first-line compliance with corporate risk policies and related exceptions, and regularly assess and make recommended adjustments as necessary or appropriate.[42] This should include reporting on significant issues related to first-line compliance with related corporate risk standards and exceptions as well.

The ERM function should also have processes in place to assess and report on the impact of the board-approved strategic business plan to the Enterprise's risk profile, and risk events that may adversely impact the achievement of strategic and business operating objectives. These processes should also include regular assessment and reporting on new business initiatives that significantly impact the Enterprise's risk profile or require regulatory review and approval. ERM should provide an aggregated view of enterprise risks and report on key risk indicators that provide a consistent view of top and emerging risk across business lines and processes. The frequency and variety of reporting should be a function of the risks, changes in the risks, and impact to decisions.

Related Guidance and Regulations

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

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

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

Model Risk Management Guidance, Federal Housing Finance Agency Advisory Bulletin 2013-07, November 20, 2013.

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

[41] 12 CFR Part 1239.11(c)(2) and (5).
[42] 12 CFR Part 1239.11(c)(5).

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

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

Data Management and Usage, Federal Housing Finance Agency Advisory Bulletin 2016-04, September 29, 2016.

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

Information Security Management, Federal Housing Finance Agency Advisory Bulletin 2017-02, September 28, 2017.

Cloud Computing Risk Management, Federal Housing Finance Agency Advisory Bulletin 2018-04, August 14, 2018.

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

Liquidity Risk Management, Federal Housing Finance Agency Advisory Bulletin 2018-06, August 22, 2018.

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

Interest Rate Risk Management, Federal Housing Finance Agency Advisory Bulletin 2018-09, September 28, 2018.

Business Resiliency Management, Federal Housing Finance Agency Advisory Bulletin 2019-01, May 7, 2019.

Enterprise Fraud Reporting, Federal Housing Finance Agency Advisory Bulletin 2019-04, September 18, 2019.

Compliance Risk Management, Federal Housing Finance Agency Advisory Bulletin 2019-05, October 3, 2019.

Credit Risk Transfer Analysis and Reporting, Federal Housing Finance Agency Advisory Bulletin 2019-06, November 14, 2019.

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.