Federal Housing Finance Agency

ADVISORY BULLETIN

AB 2014-02: Operational Risk Management

Purpose

This advisory bulletin (AB) applies to Fannie Mae and Freddie Mac (the Enterprises), the Federal Home Loan Banks (FHLBanks), and the Office of Finance (for purposes of this AB collectively, the regulated entities). The AB describes the four basic components of a program to manage operational risk effectively: risk *identification* and *assessment*; *measurement* and *modeling*; *reporting*; and *risk management decision-making*. It also addresses governance aspects of operational risk management, *i.e.*, the duties and responsibilities of management and the board of directors.

For the Enterprises, this AB rescinds and replaces the Office of Federal Housing Enterprise Oversight (OFHEO) Enterprise Guidance on Operational Risk Management PG-08-002, dated September 23, 2008. FHFA has issued AB 2024-02 Enterprise Operational Event Reporting, dated June 28, 2024, providing updated guidance on, among other things, collecting data about operational risk events and reporting such events to FHFA.

Background

In its examination rating system (CAMELSO[1]) and its Prudential Management and Operations Standards (PMOS[2]), FHFA identified matters examiners may assess when evaluating a regulated entity's management of its operational risk. This AB provides further guidance to the regulated entities on the effective management of operational risk and is intended to promote the safety and soundness of the regulated entities by providing specific guidance upon which each regulated entity should manage operational risk. To be effective, a regulated entity's operational risk policies, procedures and practices should: (1) reflect the complexity, operations, conditions and

[1] AB 2012-03 FHFA Examination Rating System (December 19, 2012).
[2] 12 CFR part 1236, Appendix A.

strategic plans of the regulated entity, as well as the economic and legal environment within which the regulated entity conducts business; and (2) be appropriate for the scale and nature of the regulated entity's business.[3] FHFA expects that each regulated entity's operational risk management program will evolve over time, just as industry and supervisory standards such as the work of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission and the Basel Committee on Banking Supervision have evolved.

Sound management of operational risk includes developing and applying operational risk management policies, procedures, and processes consistently across the regulated entity. A regulated entity's operational risk management program should conform to professional practices, comply with regulatory requirements, and achieve results consistent with the regulated entity's objectives.

The scope of the operational risk management program should encompass:

- Risk *identification* – including defining operational risk;
- Risk *assessment* – including analysis of the severity and likelihood of operational events given the effectiveness of controls in place;
- *Measurement* – including the direction and magnitude of changes in risk profile and may include *modeling* – including the treatment of diverse loss types in a common and analytical framework;
- *Reporting* – including operational event reporting that provides timely and actionable information to management; and
- *Risk management decision-making* – including evidence that management decisions about operational risk mitigation strategies are informed by data and information gathered in the other processes of the program.

A regulated entity should establish: (1) an operational risk management culture across the regulated entity to identify and address operational risks; and (2) a measurement system that quantifies operational risk. The regulated entity's overall risk management program should integrate operational risk management processes. An effective operational risk management program should result in demonstrable benefits to the regulated entity, including managers and staff at the regulated entities identifying and economically managing operational risks.

Guidance

A. Components of Operational Risk Management

Effective operational risk management includes four key components:

[3] For example, the limited nature of the business of the Office of Finance will result in operational risk policies, procedures and practices that are significantly different from those of either the FHLBanks or the Enterprises.

1. Identification and assessment;
2. Measurement and modeling;
3. Reporting; and
4. Risk management decision-making.

Each of these components is described below.

1. Identification and Assessment

Before identifying and assessing operational risk, a regulated entity needs to define and effectively communicate across the regulated entity what is meant by "operational risk." At a minimum, the regulated entity's definition should consider the definition adopted for purposes of this bulletin; specifically, operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. The regulated entity's definition should encompass risks related to housing mission-related activities, including activities related to affordable housing programs or goals. The regulated entity should formulate its definition of operational risk to communicate clearly the elements of risk that are and are not included within its definition of operational risk. That definition should fit into the regulated entity's overall risk management framework so that all significant risks that the entity is exposed to can be appropriately managed. As part of its role in overseeing and assessing management's efforts to implement a common risk language and a risk awareness culture across the regulated entity, the regulated entity's board of directors should review and approve the definition of operational risk as part of its approval of the regulated entity's operational risk management policy.

The regulated entity should develop processes and mechanisms to assist in identifying operational risks. These should be appropriate for the scale and nature of the regulated entity's business, operations, and condition. According to current best practices of risk management, these processes and mechanisms generally should include risk-control self-assessments (RCSA), key risk indicators (KRIs), and key performance indicators (KPIs).

The regulated entity's assessment of operational risk should include processes that evaluate both the severity and likelihood of operational events and give consideration to the quality of controls and infrastructure that are designed to prevent, avoid, or reduce the likelihood of operational events from occurring and their impact should they occur. The regulated entity should have a process for assessing changes in the business environment and its impact on operational risk. This should include assessing the impact of changes in the volume and complexity of the regulated entity's operations due to developments in the financial, legal, and regulatory environment. The regulated entity should establish a process to identify and assess the level and trends in operational risk and related internal control structures. Assessments should be current and comprehensive (*i.e.*, address the factors listed in the Operational Risk section in AB 2012-03

of CAMELSO, and the standards related to operational risk in PMOS) across the regulated entity. The regulated entity's process for risk assessments should be sufficiently flexible to accommodate increasing complexity, new activities, and changes in internal control systems.

Details on FHFA expectations related to the sources for identifying operational risk follow.

a. *Internal Operational Event and Loss Data* – A regulated entity's operational risk measurement system should incorporate event and loss data derived from an operational event tracking system. The database may draw upon multiple sources of information including business-line level databases that report and/or track exceptions and issues. Definitions and scope of critical information that feed into the operational event database should be consistently applied across the regulated entity. The database should ultimately include operational event and loss data covering a meaningful time span, normally five or more years. Data, even if deemed 'stale' because of implementation of a new control or other management action, should not be discarded since it remains relevant for other uses such as scenario analysis, regulatory compliance reporting, and "lessons learned" materials for management. In addition, operational events are often complex and evolutionary and, thus, events that are apparently unconnected or contained may turn out to have further ramifications or be tied to subsequent events.

b. *Business Environment Assessment* – A regulated entity's operational risk measurement system should incorporate a process for assessing changes in the business environment and the impact on operational risk. This should include assessing the impact of changes in the volume and complexity of the regulated entity's operations caused by developments in the financial, legal, and regulatory environment. The regulated entity should establish a process to identify and assess the level and trends in operational risk and related internal control structures. Assessments should be current and comprehensive across the regulated entity. The process should be sufficiently flexible to accommodate increasing complexity, new activities, and changes in internal control systems.

c. *Internal Risk and Control Environment Assessment* – A regulated entity's operational risk measurement system should have a component that takes into account the condition of the internal control environment. The regulated entity may adjust measures of operational risk (including operational risk capital measures) based on measurement tools and indicators that gauge, in a forward- looking manner, improvement or deterioration in an entity's operational risk exposure and/or control environment. Sources may include internally generated KRIs and performance triggers, internal and external audit reports, examination findings and other periodic reviews such as RCSA.

d. *External Loss Data and Scenario Analysis* – Scenario analysis (identifying events that

have not occurred, but could occur at the regulated entity) and external data on industry operational loss events can be important tools of an effective operational risk management program if carefully designed and integrated into the processes and systems for risk measurement and management. The regulated entity's operational risk measurement system should include a review of external data to gain an understanding of operational loss experience of similarly sized organizations in similar lines of business. External data can complement internal operational event data as an input into a system for measuring the entity's operational risk exposure or to inform scenario analysis.

e. *Evaluation* – A timely evaluation and update of a regulated entity's operational risk measurement system is appropriate whenever the entity becomes aware of information that may have a material effect on the estimate of operational risk exposure. A complete evaluation of the entity's operational risk management program, should be conducted by a qualified, independent team of experts, staffed either internally or externally, often enough to reflect the possibility of changes in the entity's risk environment, normally at least annually.

The framework for identifying and assessing risks should be applied across the regulated entity and should be periodically reviewed and independently validated.

2. Measurement and Modeling

A regulated entity should have effective means of measuring operational risks in order to manage those risks. Management and the board of directors should establish qualitative and quantitative risk measures that indicate the direction and magnitude of the regulated entity's operational risk profile (and changes in the risk profile). Also, management and the board should have current and complete information about the limitations of those risk measures. The measures should be appropriate for the scale and nature of the regulated entity's business.

A regulated entity's internal operational risk measurement system should be supported by data about the incidence of, and losses (including potential losses) related to, operational events. The operational risk measurement system should take into account the condition of the regulated entity's internal control environment. The regulated entity may adjust measures of operational risk based on measurement tools and indicators that gauge in a forward-looking manner improvement or deterioration in a regulated entity's operational risk exposure and/or control environment. Sources of such qualitative and quantitative information could include internally gathered key risk indicators and performance triggers, internal and external audit reports, examination findings, and other periodic reviews.

The regulated entity's operational risk measurement system should include a review of external data to gain an understanding of operational loss experience at peer institutions and within the

industry. External data may serve a number of different purposes in an operational risk measurement system. For example, external data can complement internal loss data as an input into a system for measuring the regulated entity's operational risk. Even where external loss data are not an explicit input into the measurement system, such data may provide a means to assess the adequacy of the regulated entity's internal data. External data may also inform scenario analysis, provide additional data for severity distributions, or be used for validating an economic capital model. If a regulated entity incorporates scenario analysis into its operational risk measurement system, it should document the process for conducting scenario analysis including the manner in which the scenarios are generated; the frequency with which they are updated; the scope and coverage of operational loss events they are intended to reflect; and the results of the analysis and how these results impact operational risk measurement.

If a regulated entity determines its risk profile warrants modeling one or more components of its operational risk, the models should connect the real and probabilistic sides of operational risk management and treat diverse loss types in a common analytical framework.[4] The reasoning for differential incorporation of the risk assessment components in the model should be transparent and consistently applied.

Regardless of the methodologies the regulated entity uses for measuring and modeling operational risk, the measures and models should:

- Be consistent with the regulated entity's definition of operational risk;
- Use valid data acquired from reliable system(s) or process(es);
- Be periodically updated to reflect new risks;
- Be tested for sensitivity changes in data, assumptions, and model specifications; and
- Be periodically and independently validated (for example, by the internal audit function).

3. Risk Reporting

In order to carry out their respective responsibilities, senior management and the board of directors should receive regular reports with appropriate and timely information, relevant to their respective roles, related to operational risk events and the regulated entity's operational risk profile. Reports for the board of directors should provide sufficient information for the board to carry out its oversight responsibilities, and reports for management should include actionable information that supports business and risk-management decisions.

A regulated entity should have a reporting structure that provides for consistent reporting and

[4] FHFA guidance on model risk management may be found in AB 2013-07 Model Risk Management Guidance (November 20, 2013).

escalation procedures across business units and functions. The regulated entity's operational risk event reporting system should be entity-wide, rely on established reporting thresholds that do not exclude important internal operational event data, and support the assessment of the regulated entity's operational risk exposure. The particular risk profile of a business line may be considered when establishing risk limits and reporting and escalation thresholds (what is significant in one business line may not be in another), but the establishment of and adjustments to thresholds and limits should be a systematic procedure applied consistently across the regulated entity.

While the level of detail in reports to the board of directors and management may vary, reports to both about operational risk would normally be expected to address, at a minimum:

- Significant operational loss events in the prior quarter, including near misses;
- Significant changes, including to the regulated entity's business environment that may signal actual or potential increased or decreased risk of future losses;
- Significant changes to the regulated entity's processes or resources, including comparisons to previous reports and using specific indicators or metrics; and
- Policy and risk tolerance exceptions.

4. Risk Management Decision-Making

Effective operational risk management includes making decisions, when appropriate, based on operational risk identification and assessment, measurement and modeling, and reporting. Such decisions may include, for example, deciding to avoid, transfer, or mitigate unwanted risk, and monitor and allocate resources appropriately to operational risks explicitly accepted.

The link between risk management decision-making and risk identification and assessment, measurement and modeling, and reporting can be demonstrated, for example, by: (1) processes that encourage effective management based on the assessment and reporting of changes in operational risk, and discourage behavior that weakens risk management or the internal control environment; or (2) an internal written communication documenting that management at the regulated entity takes the results of the operational risk measurement and reporting systems into account when making business decisions.

For example, FHFA expects that that the FHLBanks will incorporate the documented results of operational risk assessments and/or models into their retained earnings plans; and that the Enterprises will base the allocations of economic capital, in part, on documented analysis of the other components of the operational risk identification and assessment, measurement and modeling, and reporting. While the Enterprises' allocations should be consistent with the broader economic capital measurement and allocation systems, operational risk capital allocation should

be demonstrably commensurate with the operational risk in a particular area or business and should serve as an incentive mechanism to implement cost-effective controls and active management of operational risk including techniques of avoidance, transfer, mitigation, and appropriate monitoring and resource allocation for explicitly retained risks.

Consistent application of a decision framework ensures a common marginal risk/return trade-off across the firm's lines of business, translating into risk mitigation strategies and investments consistent with each other and the entity's risk policies. Choosing among available risk mitigation strategies should involve an appropriate management review informed by one or more decision frameworks such as cost/benefit analysis, estimation of risk-adjusted return on capital (RAROC), expected utility analysis, or other approaches.

The regulated entity's operational risk management decision-making should be supported by the periodic review and updating of the other components of the operational risk management program (risk identification and assessment, measurement and modeling and reporting). To facilitate improved risk management decision-making, the regulated entities should regularly and independently validate the components of their operational risk management program against changes in the internal control environment, risk profile, and external business and market developments.

B. Governance of Operational Risk Management

Five important governance components of operational risk management are: (1) an operational risk policy; (2) board oversight; (3) executive and senior management leadership; (4) operational risk officer implementation; and (5) business unit management and staff commitment.

1. Operational Risk Policy

A comprehensive operational risk management policy forms the foundation of effective operational risk management. The policy should define operational risk as well as the roles and responsibilities of key stakeholders and of entity-wide operational risk management functions. These roles and responsibilities should support and promote an operational risk management culture across the regulated entity that effectively identifies and economically manages operational risks. While the operational risk governance structure will vary depending on the scale and nature of the regulated entity's business, it should be fully integrated into the regulated entity's overall risk management governance structure and should demonstrate the status of operational risk management within the regulated entity.

The roles and responsibilities should be designed to minimize the potential for conflicts of interest, and should support:

- The prudent acceptance of operational risk;

- The efficient and consistent efforts to manage operational risk; and
- The effective and timely communication – vertically and horizontally across the entity – about operational risk exposures and management.

2. Board Oversight

The board of directors is responsible for establishing an appropriate "tone at the top" that promotes a strong and effective risk management culture, including operational risk management, at the regulated entity. The board or its risk management committee is responsible for approving the operational risk management program and overseeing that adequate resources are available and allocated to effectively manage operational risk. The board or its risk management committee should maintain awareness and understanding of the sources of operational risk, the strategies employed across the regulated entity to manage operational risk, and the level and direction of operational risk at the regulated entity. The board or its risk management committee is responsible for overseeing management's efforts to keep the level of operational risk within established limits. Specific board or board risk management committee responsibilities related to the governance aspects of operational risk management include:

- Ensuring the independent operational risk management function is at a sufficiently senior level in the organization to provide the appropriate stature for the position and support a strong risk management culture;
- Setting and/or approving operational risk limits and tolerances;
- overseeing the periodic review and independent assessment of the processes and methodologies used to identify, assess, measure, and model operational risk;
- Reviewing and analyzing regular reports from the operational risk officer and other sources on the level and composition of operational risk; and
- Holding management accountable for unacceptable results or conditions under its purview.

3. Executive and Senior Management

Executive and senior management are also responsible for fostering a tone that promotes the strong and effective management of operational risk across the regulated entity. These highest levels of management are responsible for implementing board approved strategies and policies and ensuring that controls are in place to keep operational risk within established limits and tolerances. Executive and senior management are responsible for: (1) ensuring that the operational risk policy and standards are consistently applied across the regulated entity's business lines, units, and operations; and (2) allocating sufficient resources to operational risk management functions throughout the regulated entity. Specific executive and senior management responsibilities related to operational risk management include:

- Reviewing annually (and updating as appropriate) operational risk-related policies and procedures, and submitting policies to the board for approval;
- Ensuring all staff receive appropriate training and tools to implement the operational risk management program effectively;
- Enforcing board established operational risk limits and tolerances;
- Ensuring the independent assessment of the processes and methodologies used to identify, assess, measure, and model operational risk; and reviewing the results and taking appropriate action in light of the independent assessments; and
- Preparing, reviewing, and analyzing accurate and timely regular reports on the level and composition of operational risk for decision-making and oversight, including reports on operational events, risk and control assessments, and the effectiveness of the operational risk management function.

4. Operational Risk Officer

This guidance encompasses risk-management execution responsibilities in the term "operational risk officer." It may not be necessary that there actually be an officer with that title to effectively implement this guidance. For example, the ORO functions may be carried out by the CRO, or some other configuration of officers.

The operational risk officer (ORO) is responsible for the day-to-day implementation (including the operation, maintenance, and improvement) of the operational risk management program. The ORO is independent of the business lines. The ORO works collaboratively and cooperatively with the regulated entity's business units and internal audit function. The ORO is responsible for developing, recommending, and implementing strategies for: identifying, assessing, measuring, monitoring, reporting, avoiding, transferring, mitigating, and monitoring operational risk across the regulated entity. The ORO is responsible for developing and implementing policies and procedures for operational risk management; the regulated entity's operational risk assessment methodology; and the operational event data collection and reporting system. Specific ORO responsibilities would normally include:

- Maintaining operational risk management policy and procedure documentation that identifies roles and responsibilities of executive and senior management, business unit management, internal audit, and the operational risk management function;
- Developing the regulated entity's operational risk management strategy;
- collecting and reporting operational event data that meets internal and FHFA reporting needs and requirements;
- Developing an effective analytic framework that uses operational event data for calculating operational risk exposure; and for the Enterprises, economic capital, and for the FHLBanks, retained earnings and overall capital adequacy;
- Developing and administering the self-assessment of operational risk and internal

controls for business units across the regulated entity; and
- Establishing and enforcing criteria (such as content, distribution, frequency) for management reporting of operational risk from the business units through senior and executive management to the board of directors.

5. Business Unit Management and Staff

Business unit management and staff are responsible for demonstrating a commitment to an effective operational risk management and internal control function by implementing operational risk management-related policies and procedures. They are responsible for: taking actions that are consistent with the articulated risk appetite; safeguarding resources; producing reliable management reports; complying with applicable laws and regulations; and minimizing the potential for human error and fraud. They are also responsible for using operational risk management tools such as self- assessments, and for reporting the results of such assessments as directed by the ORO.

FHFA examiners will evaluate the regulated entities' operational risk management practices as part of the annual examination.

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.