Introduction

This module applies to Fannie Mae and Freddie Mac (collectively, the Enterprises), the Federal Home Loan Banks (FHLBanks), and the Office of Finance, (which for purposes of this module are collectively referred to as the regulated entities).

Operational risk is the exposure to loss from inadequate or failed internal processes, people, and systems, or from external events. Operational risk is inherent in all products, activities, processes, and systems of the regulated entities. Sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems. Sound operational risk management practices reflect the condition, operations and activities of the regulated entity.

Risk management, in general, encompasses the process of identifying risks to a regulated entity; measuring exposures to those risks; ensuring that an effective program is in place to monitor risk exposures on an ongoing basis; taking steps to control or mitigate risk exposures; and reporting to senior management and the board on the entity's risk exposures.

As a fundamental risk management principle, an entity's board of directors should take the lead in establishing a strong risk management culture including a strong operational risk management culture that exists throughout the entire organization. Sound operational risk management practices include a three line of defense approach – business line management, an independent enterprise-level operational risk management function, and an independent review (typically conducted on a periodic basis by the entity's internal or external auditors or qualified independent parties). Because of the pervasiveness of operational risk, operational risk management function should be fully integrated into the entity-wide risk management structure.

Operational Risk Management Program

An independent enterprise level operational risk function usually complements individual business lines' operational risk activities. The degree of independence may vary from entity to entity based on an entity's size and complexity. For example, in one regulated entity a degree of independence for the enterprise-level operational risk function may be accomplished by separating duties and relying on an independent review of processes and functions, while in another, in order to be independent, the corporate-level operational risk function will have a reporting structure that is separate from the risk generating business lines and will be responsible for ongoing development and maintenance of the operational risk framework.

An operational risk management program (ORMP) can be broadly described as the set of policies and activities through which an entity manages its operational risk exposures. The ORMP should be comprehensive and documented through policies and procedures

approved by the board of directors or board committee. The regulated entities should include relevant definitions of operational risk and operational loss in their policies. Failures to adequately define, describe, and classify operational risks and losses will impact the effectiveness of the ORMP. The board of directors should periodically review the ORMP. The board of directors is responsible for overseeing that management's operational risk management policies, process, and systems are effectively implemented.

The ORMP should be supported by policies and procedures (documentation) approved by the board of directors, including the governance structures used to manage operational risk, including reporting lines and accountabilities. The board-approved documentation should define and explain the operational risk assessment tools used by the entity. The entity's operational risk appetite and tolerance and thresholds or limits for inherent and residual operational risk and approved risk mitigation strategies and instruments should also be included in the approved documentation. Also, the documentation should include the entity's process for establishing and monitoring operational risk thresholds and limits related to inherent and residual risk exposure. Descriptions of operational risk reporting and related management information systems should also be included in the relevant documentation. An important component of all ORMPs is the development and maintenance of common operational risk language and terms to improve the consistency of risk identification, exposure ratings, and risk management objectives entity-wide. A requirement for an independent review and assessment of operational risk should be included in the documentation. And finally, the operational risk management policies and procedures should be regularly updated as the operational risk profile of an entity changes. Material changes in the operational risk appetite and operational risk tolerance for a regulated entity should receive board approval.

For Fannie Mae and Freddie Mac, an important component of the framework is an operational risk capital model. The economic capital measurement and allocation for operational risk should be embedded in a larger enterprise-wide risk management framework where allocation of economic capital is proportional to the level of risk, informs decision-making, and serves as an incentive mechanism to improve controls and risk management. Mitigation decisions — including how much of any given risk exposure to retain (if any), how to finance retained exposures, and when to institute new or modified internal controls — should be based on quantitative measurements, qualitative management assessments, models, monitoring reports, and capital allocations. This cycle of activities should be regularly repeated because risk exposures change over time as both the institution and its external environment change.

Components of the ORMP

An ORMP consists of a repeating cycle of activities that includes risk identification, risk assessment, evaluation of the control environment, measurement and modeling, reporting, and the application of management strategies to control and reduce risks. Managerial policies and objectives should guide these processes to an end result that is both consistent with the overall objectives of the entity and consistently applied across

the entity's business and corporate-level units. The sequential order generally moves from risk identification to assessment and measurement and then to reporting and use of management strategies that include allocating economic capital, monitoring risk exposures, improving the internal control environment, and transferring risk via insurance and other operational risk mitigating strategies.

An ORMP should be integrated within an overall entity risk management framework and should be built upon a policy statement and related procedures, appropriate for the scale and nature of the entity's business. The four key components of an ORMP are systems of:

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

1) Operational Risk Identification and Assessment

An effective ORMP begins with defining operational risk and building tools for risk identification and risk assessment.

A. Definition of Operational Risk

FHFA defines operational risk as the exposure to loss from inadequate or failed internal processes, people, and systems, or from external events. The regulated entity's definition of operational risk should be formulated to clearly communicate what is, and is not, included in terms of risk categories. With respect to scope, the definition should, at a minimum, encompass the exposure to loss from inadequate or failed internal processes, people, and systems, or from external events.

The regulated entity's definition should be reviewed and approved by the board of directors. This definition forms the cornerstone of the ORMP because it determines the group of risks that will and will not be managed under the rubric of operational risk, and therefore what risk data will be collected, quantified, and modeled and where management attention should be focused. Once defined, this definition should be clearly communicated to all staff. Senior management commitment to and communication of a common risk language are important steps toward the development of a risk-aware culture in the firm.

B. Risk Identification and Assessment

The entity should develop processes and mechanisms to assist in identifying operational risks. These should be appropriate for the institution and should include an operational event reporting system and other appropriate management tools such as meaningful key risk indicators (KRIs) and performance triggers, and risk heat maps or scorecards of

operational risk exposures. The entity-wide process for tracking internal operational events should be closely tied to a system of prompt analysis of the underlying causes of the events and a process for incorporating this analysis as part of operational risk assessment and measurement. The institution should collect meaningful data and performance triggers that support cause-and-effect analysis and develop forward looking risk reporting tools. The framework for identifying and assessing risks should be consistently employed throughout the institution and should be periodically and independently evaluated.

Risk identification and assessment includes processes that assess both the severity and likelihood of operational events with consideration given to the quality of controls and infrastructure that are designed to prevent, avoid, or reduce the likelihood of occurrence of operational events and their impact should they occur. These internal controls should meet or surpass industry standards and be periodically reviewed as part of an effective internal risk control self-assessment (RCSA) process.

More details on supervisory expectations related to these information sources follow.

i. Internal Operational Event and Loss Data

The regulated entities should track operational events. An operational event database should be established that includes operational event and loss data covering five or more years. While past losses may not be indicative of potential future losses when new controls or changes in business strategies make particular loss events much less likely to occur, data should not be discarded since it remains relevant for other uses such as scenario analysis, regulatory compliance reporting, and "lessons learned" 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.

ii. Business Environment Assessment

The regulated entity should have 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 institution operations due to developments in the financial, legal, and regulatory environment. The 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 entity. The process established to maintain these risk assessments should be sufficiently flexible to accommodate increasing complexity, new activities, and changes in internal control systems.

iii. Internal Risk and Control Environment Assessment

The regulated entity's operational risk measurement system should have a component that takes into account the condition of its 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 institution's operational risk exposure and/or control environment. Sources of such qualitative and quantitative information may include internally gathered key risk indicators (KRIs) and performance triggers, internal and external audit reports, examination findings, and other periodic reviews such as risk control self-assessments (RCSAs). FHFA does not prescribe a specific methodology, but examiners will assess the processes used by the regulated entities to integrate qualitative and quantitative measures of the internal control environment factors into the quantification of operational risk exposure.

iv. External Loss Data and Scenario Analysis

Scenario analysis and external data on industry operational loss events can be important tools of an effective ORMP if carefully designed and integrated into the processes and systems for risk measurement and management. The entity's operational risk measurement system should include a review of external data to gain an understanding of industry operational loss experience. 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 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 institution'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 performs scenario analysis, it should document its 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 risks they are intended to reflect, and the results of the analysis and how it impacts operational risk measurement.

v. Evaluation

A timely evaluation and update of a regulated entity's operational risk measurement system is justified whenever the entity becomes aware of information that may have a material effect on the estimate of operational risk or operational risk capital allocation. A complete evaluation of the entity's operational risk measurement system, including all modeling inputs and assumptions, should be done at least annually by a qualified, independent team of experts, staffed either externally or internally.

An effective ORMP should include independent evaluation. The regulated entities may use independent and qualified internal or external parties to perform evaluations. The scope of such evaluations should be sufficient to assess the effectiveness of the ORMP and should include the activities of the firm-wide, independent operational risk

management function, and the operational risk management activities of business units and senior management.

2) Measurement and Modeling

Measuring operational risks is an important part of risk management. Providing senior management with measures of risk that indicate the direction and magnitude of changes in the risk profile is essential, but senior management should also know the limitations of these risk measures. Models of operational risk are often used to connect the real and probabilistic sides of operational risk management and to treat diverse loss types in a common analytical framework.

The methodologies used to measure operational risk should:

1) Be consistent with an entity-wide definition of operational risk that encompasses FHFA's definition as stated above (*see* Definition of Operational Risk);
2) Use valid data derived from an adequate data collection system to support the metrics and assessments of risk;
3) Be tested for sensitivity to changes in data, assumptions, and model specification; and
4) Be periodically and independently validated.

In addition to meeting these criteria, the entity's operational risk measurement system should include the following components:

1) Internal operational event data;
2) Forward-looking business environment assessment;
3) Internal risk and control assessments;
4) External event data; and
5) Scenario analysis (identifying events that have not, but could occur at the regulated entity).

For the Enterprises, operational risk measurement system should support the determination and allocation of economic capital for operational risk. This determination could encompass a statistical model, hypothetical events, data from actual events at the Enterprise, and/or data from pertinent operational events at other similar financial institutions. However, the quantity and quality of the internal and external event data, the risk profile, and the internal control environment of the Enterprise will influence the weight placed on certain components. For example, there may be cases where estimates of operational risk based primarily on internal and external loss event data would be unreliable for business lines with a heavy-tailed loss distribution and a small number of observed losses. In such cases, scenario analysis and business environment and control factors may play a more dominant role in the risk measurement system. Conversely, operational loss event data (internal and external) should play a more dominant role in the operational risk economic capital model for business lines where data are deemed

reliable. The reasoning for differential incorporation of the risk assessment components in the model must be transparent and consistently applied.

3) Reporting

A. Regular Reporting Structure

The effectiveness of the ORMP depends upon the dynamic processes of risk identification and assessment, measurement, and management response, facilitated by the risk reporting process. For management to understand the status of the entire risk management system over time, a systematic reporting structure should be developed. Reports should provide timely and actionable information to management. The entities should have a framework that provides for consistent reporting and escalation procedures across the business units and functions. 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 institution.

Regular reporting of pertinent information to senior management and the board of directors supports the proactive management of operational risk. Risk reporting should present management with information they can use to take actions; the purpose of risk reporting is to support business and risk management decisions.

B. Information Reported

Reports to senior management should include, at a minimum:

1) Significant operational events in the prior quarter, including events that did not necessarily result in financial losses yet were significant control or process breakdowns;
2) Factors signaling increased or decreased risk of future losses;
3) Significant changes in the state of the regulated entity's processes and resources, with comparison to the previous report using specific indicators or metrics; and
4) Changes to risk policies, limits, or tolerance levels.

4) Risk Management Decision-Making

Operational risk management goes beyond implementing effective controls and requires positive decision-making to manage risks. Operational risk might be addressed through effective techniques of avoidance, transfer, mitigation, and appropriate monitoring and resource allocation for explicitly accepted risks. Controls throughout the regulated entity should meet industry standards, and examiners should evaluate the effectiveness of

mitigation measures, both in terms of control-oriented approaches to prevent the occurrence of events, and insurance programs to limit the severity of events that occur.

Choosing among available risk-mitigation strategies should involve 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. Application of the decision framework ensures a common marginal risk/return trade-off across the firm's lines of business translating into risk mitigation strategies consistent with each other and the entity's risk policies.

Operational Risk Governance: Management Responsibilities and Duties

The ORMP should define the roles and responsibilities of key players and of corporate-wide functions. In addition to a chief operational risk officer, or individual with equivalent duties, key players include senior management and the board of directors, a chief risk officer, a risk oversight committee, business unit managers, and individuals from corporate-wide functions, including risk management, treasury, internal audit, legal, human resources, and information technology.

The importance of operational risk management in the corporate culture is reflected in the structure of the ORMP and its relationship with other areas of management. Managers of the operational risk management function should be of sufficient stature to perform their duties effectively. This is usually evidenced by position titles and authorities that are comparable to the titles and authorities of other risk management functions, including credit and market risk. In addition, operational risk management functions must be held by individuals with relevant operational risk management experience and technical capabilities in order to be credible.

Other important structural elements include the reporting relationship between corporate operational risk management and business units, other corporate-level units, and the distribution of responsibility and authority for taking and managing operational risks. Employee training, position requirements, performance evaluations, and incentive structures all should support the effective implementation of the ORMP. The allocation of roles and responsibilities across the firm is important because they determine (a) the incentives to take and manage operational risks; (b) the efficiency and consistency of risk management efforts; (c) the potential for conflicts of interest; and (d) the level of horizontal and vertical communication about operational risk exposures and their management.

The regulated entity's risk management decision-making should reflect the other parts of the ORMP (risk identification and assessment, measurement and modeling, and reporting). This is commonly referred to as a "use test," meaning that the components of the ORMP are actually implemented, or put to use, and trigger the appropriate management response. The regulated entity's ORMP should:

1) Not be limited to regulatory requirements;
2) Evolve as the entity gains experience with operational risk management strategies and results; and
3) Provide benefits to the entity in the management and control of operational risk.

The ORMP should include processes that encourage effective management based on the assessment and reporting of changes in operational risk and processes that discourage behavior that weakens risk management or the internal control environment. The regulated entity should periodically review and update the operational risk event collection, reporting, and measurement systems to reflect changes in the internal control environment and external business and regulatory context.

The FHLBanks should incorporate operational risk assessments and/or models into their retained earnings plans. The Enterprises should be able to demonstrate the impact that the allocation of operational risk capital has on its decision-making. While this allocation should be consistent with the broader economic capital measurement and allocation systems, operational risk capital allocation should be 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.

Each level of governance has certain roles and responsibilities within the ORMP. FHFA examiners will assess whether an entity has assigned and executed responsibilities for ORMP that are equivalent to, or achieve the same desired outcome as, those described below.

A. Board of Directors

The board of directors is responsible for establishing a "tone at the top" that promotes a strong risk management culture. This requires that the board approve the ORMP and ensure that adequate resources are available to manage operational risk. The board should clearly communicate throughout the institution the need to be fully informed of, and to understand the sources of, operational risk and the strategy to be employed to address that risk.

In order to maintain a "tone at the top" that supports operational risk management, the board should demonstrate interest and visible support by actively engaging management on issues related to the identification, assessment, and management of operational risks at the entity.

Specific responsibilities of the board relate to:

i. Risk Management Function

The board should approve the establishment of a firm-wide independent operational risk management function within the entity that will be responsible for the day-to-day

implementation of the ORMP. While that function may be housed within another risk management department, the board should also establish clear lines of management responsibility and accountability for implementing a strong risk management environment.

ii. Policy

The board should review and approve the implementation of an ORMP and subsequent major changes. It should review and approve the policy provisions that establish the major framework elements and management's plans to implement the ORMP, including identifying and assessing, measuring, monitoring, and managing risk. While management's role is to ensure that procedures implementing the ORMP are developed and are effective, the board must be given sufficient information to understand and approve the ORMP and any significant changes to it. The board should ensure that management has incorporated professional best practices into the ORMP, and that management has procedures in place to identify changes in the external environment, or risks from new activities, that, once identified, are to be reflected in the ORMP as appropriate.

iii. Resource Allocation

The board should ensure that sufficient resources are allocated to the management of operational risk.

iv. Compensation Programs

The board should ensure that the effectiveness of the regulated entity's operational risk management is reflected in the performance evaluations and compensation of senior management.

B. Senior Management

Senior management should be actively involved in ensuring that the ORMP is implemented and consistently applied across the institution. This includes developing for board approval a strong governance structure with well-defined lines of responsibility, and establishing and maintaining robust challenge mechanisms and issue-tracking processes designed to escalate issues as necessary to ensure resolution. Senior management is responsible for implementing and maintaining policies, processes, and systems for managing operational risk. In addition, senior management has the following areas of responsibility:

i. Culture

For the ORMP to be effective, senior management should set an appropriate tone of commitment to the goal of effective operational risk management, consistent with that of the board of directors, and ensure that all levels of staff clearly understand their roles and

responsibilities for operational risk management within the entity, the sources of operational risk, and the entity's operational risk management strategies.

ii. Allocation of Resources

Senior management must allocate the resources among the firm-wide operational risk management function, the business units, and internal audit to effectively implement and operate the ORMP.

iii. ORMP Oversight

Senior management should annually review and update as appropriate the ORMP and related policies. Material changes must be approved by the board. In addition, senior management should review reports on operational events, risk and control assessments, and risk measurement to assess effectiveness of the ORMP.

C. Operational Risk Officer

An independent entity-wide operational risk officer appointed by senior management or the board of directors should be responsible for the day-to-day implementation of the ORMP. Depending upon the size and complexity of the regulated entity, this function might be in a standalone unit or housed within another risk management function. The individual in this role should have equivalent senior management status and clearly designated duties that include developing and recommending strategies for identifying, assessing, monitoring, and controlling/mitigating operational risk on a firm-wide basis. The operational risk officer should also oversee the operation, maintenance, and improvement of the components of the ORMP once they have been established. The status and additional duties of the operational risk officer are further elaborated below:

i. Independence

The operational risk officer should have functional independence from the business units and from internal audit, but should operate in a cooperative and collaborative manner with these entities.

ii. Operational Event Data Collection

The operational risk officer should lead a process for the collection and reporting of operational event data that meets internal reporting needs and applicable FHFA reporting requirements.

iii. Documentation of Policies and Procedures

The operational risk officer is responsible for maintaining documentation of policies and procedures for the ORMP. Operational risk management documentation should identify roles and responsibilities of senior management, business unit management, internal audit, and the operational risk management function. The documentation should provide definitions of operational risk and operational event types. The documentation should describe the regulated entity's operational risk management strategy, the use of internal and external operational event data, and the analytic framework for calculating operational risk exposure and economic capital. In addition, the entity should document its process for the self-assessment of operational risk and internal controls by business units.

iv. Reporting

The operational risk officer should oversee management reporting of operational risk from the business units through senior management to the board of directors. Such documentation should include report content, distribution, and frequency.

D. Business Line and Administrative Unit Management

Business line and administrative units are best situated within the entity to understand the drivers of operational risk and the most effective methodologies to control and mitigate that risk. Operational risk management should reinforce business line and administrative unit commitment to an effective risk management and internal control structure that:

1) Reflects risk taking, risk management decisions, and operational risk controls consistent with the institution's risk appetite as approved by the board of directors;
2) Safeguards resources;
3) Produces reliable management reports;
4) Complies with applicable laws and regulations; and
5) Minimizes the potential for human error and fraud.

Business line and administrative unit management should periodically self-assess the use of ORMP tools, the effectiveness of risk management policies and procedures, as well as the internal control system, and report such assessments to internal audit and the independent operational risk management function.

Regulatory Environment

The primary authorities governing or relevant to operational risk are set forth below. The examiner should ensure that the application of such authorities to a regulated entity has been considered by the regulated entity and its legal counsel.

1) Rules and Regulations of the Federal Housing Finance Agency (FHFA)

12 CFR part 1236 FHFA's Prudential Management and Operations Standards (PMOS) –Standard 1 (Internal Controls and Information Systems), Standard 4 (Management of Market Risk—Measurement Systems, Risk Limits, Stress Testing, and Monitoring and Reporting), Standard 8 (Overall Risk Management Processes). Standard 1 regarding internal controls and information systems states that the board of directors and senior management should ensure that the regulated entity has an effective internal control system that defines controls at every business level. In addition, a regulated entity should have information systems that provide relevant, accurate, and timely information and data.

Standard 4 requires the institution to maintain measurement systems capable of valuing all financial assets, including derivatives. In addition, Standard 4 dictates that the regulated entity has risk monitoring and reporting systems that provide regular, accurate, informative, and timely market risk reports.

Standard 8 (Overall Risk Management Processes) requires each regulated entity to have an independent risk management function, or unit, with responsibility for risk measurement and risk monitoring, including monitoring and enforcement of risk limits. PMOS Standard 8 states that the CRO should head the risk management function and should report directly to the CEO and the risk committee of the board of directors.

2) Rules and Regulations of the Federal Housing Finance Board (Finance Board), which include the following section relevant to the FHLBank's operational risk management:

12 CFR 932.6 defines the operations risk capital requirement.

12 CFR 917.3 describes requirements for risk management policy, including an effective internal control system which is described in 12 CFR 917.6.

3) Advisory Bulletins of the Finance Board that provide supervisory guidance relating to the topic of operational risk management include the following:

Advisory Bulletin 99-6, dated May 7, 1999, Framework for Internal Control Systems, provides guidance on assessing the framework for internal control systems.

Advisory Bulletin 03-5, dated April 16, 2003, Annual Risk Assessments, provides guidance on annual risk assessments required by 12 CFR 917.3(c).

Advisory Bulletin 04-01, dated March 10, 2004, Service Organizations, provides guidance on FHLBanks' use of service organizations to perform critical activities for FHLBank operations, particularly Acquired Member Assets programs.

4) Office of Federal Housing Enterprise Oversight (OFHEO) policy guidance relating to operational risk management:

Enterprise Guidance on Operational Risk Management (PG-08-002), dated September 24, 2008, sets forth standards for the operational risk management programs of Fannie Mae and Freddie Mac.

5) Other Guidance related to the Enterprises' operational risk management practices includes:

Operational Event Data Collection and Reporting Requirements, correspondence August 10, 2007, FNM OPAR-2007-003, FRE OPAR-2007-53.

Issues Specific to the Enterprises

1) <u>Operational Risk Economic Capital</u>

The operational risk officers at Fannie Mae and Freddie Mac should have responsibility for establishing an analytic framework that supports the calculation and allocation of economic capital for operational risk. Entity risk management and economic capital allocation systems and the respective operational risk officer should work with senior management to ensure that the allocation of operational risk economic capital is consistent and supportive of effective risk management. Operational risk at Fannie Mae and Freddie Mac should be calculated on a periodic basis and reported to business unit managers, senior management, and the board of directors.

FHFA may review Fannie Mae and Freddie Mac allocations of economic capital for managing operational risk. Such reviews should focus on understanding the behavioral effects of the allocation, such as incenting management to take steps to reduce operational risk, as well as reviewing the measurement system that generates the economic capital calculations and allocations across the entity.

2) <u>Instructions for Operational Event Data Collection and Reporting</u>

For purposes of operational risk management and measurement, the regulated entities should track the incidence of, and losses related to, operational events. FHFA's expectations regarding systems for collection and reporting of internal operational events and losses for the Enterprises are contained in *Instructions for Operational Event Data Collection and Reporting* (Instructions). The Instructions include regulatory reporting instructions and requirements for an operational event and loss data collection and reporting system. By imposing a common taxonomy for operational event data reporting that includes risk definitions, terminology, and classifications, FHFA ensures consistency and comparability in reporting to properly assess the status and trends in operational risk.

For operational risk management purposes, FHFA defines operational losses to include all direct and indirect economic losses, including those related to legal liability, reputational setbacks, and compliance and remediation costs to the extent that such costs are direct consequences of operational events. However, operational losses do not include costs generally related to risk management and enhancements to controls, systems, and processes to prevent future operational losses.

FHFA recognizes that accurately calculating certain losses from operational events can be difficult, particularly with regard to certain opportunity costs and indirect losses. Therefore, the Instructions do not require the estimation and reporting of such losses. For operational risk management purposes, however, FHFA expects those losses to be considered in the ORMP.

Issues Specific to the FHLBanks

1) Risk-Based Capital

12 CFR 932.6 establishes the operational risk capital requirement. The requirement is equal to 30 percent of the sum of the FHLBank's credit and market risk capital requirements. Section 932.6 also allows an FHLBank to substitute an alternative methodology for calculating operational risk if such methodology is approved by the FHFA.

Examination Guidance

The workprogram for the Operational Risk Management (ORM) examination module is detailed below. If this module is included in the examination scope, the examiner must perform worksteps sufficient in coverage to document the basis for the conclusions on the quantity of risk and quality of risk management pertaining to this area. Transaction testing is mandatory and the examiner must document sufficient worksteps from Section 4, *Testing*, to support the findings and conclusions from this examination module.

In determining the extent of review and testing to be conducted in completing each examination, the examiner should take into account applicable FHFA off-site monitoring or analysis reports, such as analyses on the quality and effectiveness of corporate governance practices, financial condition and performance, economic and housing industry conditions, internal controls, and audit coverage relating to the entity's operational risk management activities.

NOTE: Text in (*italics*) referenced in a workstep represents illustrative guidance that serves as suggestions for specific inquiry.

1. Scope of Examination Work Performed

1) Review past reports of examination for outstanding issues or previous problems related to operational risk management.

2) Review FHFA off-site monitoring or analysis reports, and workpapers produced as part of on-going monitoring, related to operational risk management.

3) Assess the status of outstanding examination findings pertaining to operational risk management.

4) Review internal audit reports for outstanding issues relating to operational risk management.

5) Review minutes of meetings of the board of directors and relevant board and management committees for any issues regarding operational risk management.

6) Evaluate key operational risk personnel and reporting lines.

7) Has the regulated entity's board of directors approved an operational risk management (ORM) policy?

8) Has the regulated entity developed an operational risk management program?

9) Is there a chief operational risk officer (CORO) or an identified individual with equivalent responsibilities?

10) Is the stature of the position equal to other similar risk officers within the entity?

11) Are the duties and responsibilities defined in a job description?

12) Are the CORO's responsibilities consistent with those of other risk officers within the entity?

13) Is the CORO responsible for overseeing management reporting of operational risks from the business units through senior management to the board of directors?

14) Do ORM managers, including the CORO or equivalent, have appropriate skills and operational risk management experience to effectively engage with the business line on operational risk related issues?

15) Has the board of directors (or relevant committee) reviewed and approved the charter and framework for the ORM function, including goals and objectives for the function?

16) Does senior management ensure that the Operational Risk Management Framework is consistently applied across the regulated entity?

17) Are all entity employees informed of their responsibilities for operational risk management? Are they trained in identifying sources of operational risk?

18) Is the ORM program designed to identify and mitigate or manage operational risks?

2. Description of Risks

1) Has the entity established risk identification systems and measurement processes that accurately identify and aggregate operational risks across the entity?

2) Has the entity developed useful key risk indicators (KRI's), metrics, and related performance measures for operational risk?

    a) Are the businesses sufficiently involved in the development of the KRI's so that they are useful and relevant indicators of operational risk?

b) Are the indicators regularly and routinely used to track and report on operational risks?

3) Does the entity maintain an entity-wide process to collect, analyze, and report on internal operational events and losses? Do the Enterprise's systems comply with FHFA letters to the Enterprises regarding "Instructions for Operational Risk Event Data Collection and Reporting" (August 10, 2007; FNM OPAR 2007-003, FRE OPAR 2007-53) including regulatory reporting instructions, operational event and loss data collection, and reporting?

4) Do business unit personnel or ORM personnel conduct periodic risk assessments that identify business line operational risks?

5) Are these risk assessments reviewed for thoroughness and accuracy by ORM personnel?

6) Has reporting related to the risk assessment process been established? Does it include aggregating (consolidating) and analyzing entity-wide operational risks identified through the risk assessment process? Is this information regularly reported to senior management and the board of directors?

7) Does documentation support management's decision to accept or mitigate operational risks identified and reported through the operational risk assessments?

8) Has the entity implemented an operational risk scenario process or function?

   a) Is the process for conducting scenario analysis documented, including a description of the development of the scenarios, the update frequency, and the scope and coverage of operational loss events they are intended to cover, and how the scenarios impact operational risk measurement?
   b) Are the results of the scenarios documented and analyzed?
   c) Do the policies and procedures for the scenario process require that external data on industry operational events are included in the process?
   d) Is the scenario analysis incorporated into the entity's operational risk management system?

9) Has the entity developed a reliable root cause analysis process to evaluate operational related issues?

   a) Are findings from root cause analysis documented and shared with senior management and relevant business managers?

10) Has the entity established methodologies to measure its operational risks? (Note: Fannie Mae and Freddie Mac have established operational risk modeling methodologies for economic capital measurement purposes. The economic capital

allocation related to operational risk should be proportional to the enterprise's level of risk and embedded in the enterprise-wide economic capital framework.)

a) If so, are the methodologies tested for sensitivity and changes in data, assumptions or model specifications?
b) Are they periodically independently validated?
c) Does the measurement system include internal operational event data, forward looking business environment assessments, external event data and scenario analysis?
d) Does the entity's operational risk measurement system support their calculation and allocation of economic capital for operational risk?
e) Does the measurement system incorporate a component that takes into account the condition of the entity's internal control environment?
f) Is the entity's operational risk measurement system periodically reviewed and updated?

3. Risk Management

Risk Identification Process

1) Has the entity implemented processes and techniques to avoid, transfer, or mitigate known operational risks?

2) Is there a process to test and report on the adequacy of the entity's internal controls?

3) Does the entity maintain insurance coverage to mitigate losses related to operational events? Is the level of insurance coverage monitored on a regular basis?

4) Does the entity use risk mitigation strategies that employ a decision framework such as cost/benefit analysis or a risk adjusted return on capital analysis?

Organizational Structure

1) Review the current ORM organizational chart.

a) Evaluate the effectiveness of the organization by considering the reporting lines for key operational risk personnel.
b) Does the CORO report to executive management and board of directors?
c) Is the reporting structure between the operational risk management function and business units clearly described and defined?
d) Is the CORO functionally independent of the business units and internal audit?

e) Have significant management, personnel or organizational changes occurred within the enterprise-wide risk management function including the ORM?

2) Evaluate the resources allocated to ORM.

a) Is staffing adequate? Consider staffing levels, seniority and expertise.
b) Are ORM personnel qualified to effectively engage with the business line on operational risk related issues? Consider experience, seniority and stature within the entity.

Policy and Procedure Development

1) Has the entity established adequate ORM policies and procedures that are approved by the board of directors (or relevant committee)?

a) Do the policies require updating to reflect changes in the entity's business?
b) Do the policies assign the responsibility and authority for taking and managing operational risk?
c) Do the policies and procedures describe the risk management tools and techniques that the entity will use to identify, track, and manage operational risks?
d) Do the policies articulate a common risk language for the entity such as high, medium, and low levels of risk?
e) Do the policies contain the entity's definition of operational risk? Was the operational risk definition specifically approved by the board of directors? Has the definition been communicated across the entity's business lines?
f) Do the policies contain the entity's definition of an operational loss?
g) Do the policies include an operational risk appetite and a risk tolerance statement? Are the nature, types, and levels of operational risk that the entity is willing to assume articulated?
h) Do the policies contain approved risk mitigation strategies?
i) Are the policies consistent with other enterprise-wide risk management policies?
j) Do the policies and procedures define the roles and responsibilities of key officers and employees related to operational risk management?
k) Do the ORM policies and procedures address changes in business activities or operations, including things such as new products and activities? Are such changes defined in the policies? Do the policies describe the process for analyzing and evaluating operational risks related to these changes including potential impacts on staffing, internal controls, technology, operations, accounting, and financial disclosure? Does the policy require "signoffs" by the areas within the entity that will be impacted by the change such as enterprise-wide risk management, accounting, internal controls, legal, technology, internal audit, and senior management?

Reporting

1) Are executive management and the board of directors provided with sufficient information to understand the operational risks faced by the entity?

    a) Does the entity regularly produce and provide to executive management and the board of directors operational risk reporting that is accurate, effective, and relevant?
    b) Do entity-wide operational risk exposures receive the appropriate level of attention from the board of directors and executive management?
    c) Does the entity maintain a process to effectively escalate operational risks to senior management and the board of directors?
    d) Is operational risk reporting integrated with other enterprise-wide risk reporting so that the board of directors and senior management receive a consolidated view of enterprise-wide risks?
    e) Does operational risk management reporting include the identification, description, and prioritization of operational risks?
    f) Does ORM reporting include trend analysis?
    g) Is the reporting format consistent and does it facilitate tracking of improving or deteriorating operational conditions at the entity?
    h) Does the reporting contain an assessment of the adequacy of internal controls and identify internal control weaknesses?
    i) Does the reporting describe systems and process capabilities including capacity?
    j) Does the reporting identify information systems issues including an analysis of the root causes of any problems? Does the reporting provide information on how well information systems function and either contribute to or mitigate operational risks at the entity? Does the reporting contain information addressing the adequacy of the entity's business resumption activities?
    k) Does reporting contain information on the significant operational losses identified during the prior quarter and include an analysis and description of the root cause of the losses?

Internal/External Audit

1) Does the entity's internal audit function independently review the entity's ORM program including testing for compliance with the policies and procedures?

    a) Do audit procedures require, and reports include, an evaluation of the independence and effectiveness of operational risk management program?
    b) Does internal audit opine on the overall appropriateness and adequacy of the entity's ORM framework?
    c) Does internal audit review the entity's process for setting the operational risk appetite and tolerance level?

d) Does internal audit review the process for constructing and also test the reliability of operational risk management oversight reports provided to executive management and the board of directors?
e) Are ORM related audit findings resolved by management in a timely manner?

Compliance

1) Assess compliance with FHFA's PMOS standards, including Standard 1 (Internal Controls and Information Systems), Standard 4 (Management of Market Risk—Measurement Systems, Risk Limits, Stress Testing, and Monitoring and Reporting) and Standard 8 (Overall Risk Management Processes).

4. Testing

1) Review the entity's ORM framework. Determine if the major components of a standard ORM framework have been implemented by the entity. If major components of a standard ORM framework have not been established, determine why. Major components of a standard framework include the following:

   a) Common risk language.
   b) Risk assessment tools including operational event and loss collection.
   c) Key risk indicators and metrics.
   d) Internal risk and control assessment process.
   e) Business environment assessment process.
   f) External loss data.
   g) Scenario analysis.
   h) Root cause analysis.
   i) An operational risk measurement process.
   j) Risk mitigation methodology.

2) Perform a "Use Test" to confirm that the entity's ORM framework is not limited to satisfying the regulatory requirement to establish an operational risk management program. Identify tangible benefits to the entity from the operational risk management program. Benefits may include stronger internal controls, the reduction of business continuity risks, and more efficient operational processes.

3) Identify a small sample of reported operational risk losses or operational risk events. Trace the remediation of the events to determine that the issues that contributed to the loss or a break down are resolved. If the issue is not resolved determine if there is satisfactory reason the situation was not resolved.

4) Obtain the most recent operational risk reporting provided to the board of directors. Determine if the reporting accurately portrays the operational risk environment at the

entity. Does the reporting aggregate the entity's operational risk in an understandable way? Does the reporting include descriptions of recent operational losses or events? Select an appropriate sample of items in the reporting and trace these items to supporting documentation.

5) Select an appropriate sample of risk and control self-assessments (RCSAs). Evaluate the adequacy, consistency, and timing of the RCSAs. Determine if the policies or instructions for conducting RCSAs were followed. Assess that conclusions concerning risks identified in the RCSAs are reasonable. If issues were identified through the assessment process, have they been addressed?

6) Evaluate the adequacy of the objectives and scopes of reviews conducted by third party consultants and determine the status of management actions regarding any recommendations stemming from the reviews. Determine if management's actions were adequate.

7) Review the resumes and job descriptions of ORM personnel. Determine if they possess the necessary education, experience, training, and professional certifications to effectively carry out their responsibilities.

5. Conclusions

1) Summarize conclusions for all examination work performed, including work performed by other FHFA staff as it relates to operational risk management practices. Develop a memorandum articulating the risks to the institution resulting from weaknesses identified. The memorandum should describe the basis of conclusions reached and summarize the analysis completed. Within the memorandum, discuss the operational risk the regulated entity is exposed to; the level of risk exposure; the direction of risk (stable, decreasing, increasing); and the quality of risk management practices (strong, adequate, weak). A memorandum must be prepared irrespective of whether the examiner's assessment is positive or negative. The memorandum should include a recommended rating for the Operational Risk component consistent with the FHFA examination rating system.

2) Conclude on the responsiveness to previous examination findings. Evaluate the adequacy of the regulated entity's response to previous examination findings and concerns.

3) Develop findings and prepare findings and analysis memoranda, as appropriate. Based on examination work performed, develop findings communicating concerns identified during the examination. Findings should identify the most significant risks to the institution and the potential effect to the regulated entity resulting from the

concerns identified. Such documents should describe a remediation plan specifying the appropriate corrective action to address examination concerns and establish a reasonable deadline for the regulated entity to remediate the finding. Communicate preliminary findings to the EIC. Discuss findings with regulated entity personnel to ensure the findings and analyses are free of factual errors.

4) Develop a list of follow-up items to evaluate during the next annual examination. In addition to findings developed in the steps above, include concerns noted during the examination that do not rise to the level of a finding. Potential concerns include issues the regulated entity is in the process of addressing, but require follow-up work to ensure actions are completed appropriately. In addition, potential concerns should include anticipated changes to the institution's practices or anticipated external changes that could affect the institution's future operational risk management practices.

Workprogram

1. Scope of Examination Work Performed

Workpapers must document the examination activities undertaken to evaluate potential risks related to operational risk management.

2. Description of Risks

- Identify areas of concern related to operational risk management
- Assess current risks and trends in the risk to the organization emanating from the operational risk management area
- Evaluate changes within the organization or industry affecting operational risk
- Evaluate the entity's own risk-identification practices and conclude on their adequacy

3. Risk Management

- Assess and conclude on the adequacy of the organization's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
    - The regulated entity's organizational structure
    - Policy and procedure development for operational risk management
    - Appropriateness of risk metrics established for operational risk management
    - Reporting by management and the board
- Assess and conclude on the internal and external audit of operational risks
- Assess and conclude on the adequacy of information technology and controls related to operational risk management
- Assess and conclude on the adequacy of the organization's efforts to ensure:
    - Compliance with laws, regulations and other supervisory guidance
    - Compliance with the organization's policies and procedures

4. Testing

- Complete testing, as appropriate, to assess adherence with applicable standards

5. Conclusions

- Summarize conclusions for all examination work performed related to operational risk management
    - Conclude on the level of risk to the organization
    - Include an assessment of the adequacy of an organization's monitoring of operational risk and establishment of internal controls to mitigate risk
- Conclude on responsiveness to examination findings from previous examinations
- Develop examination findings as appropriate
- Identify areas requiring follow-up examination activities or monitoring