THE OFFICE OF FEDERAL HOUSING ENTERPRISE OVERSIGHT (OFHEO)

Enterprise Guidance on Operational Risk Management (PG-08-002)

Approved____________________ Date: 9/23/08

James B. Lockhart III

Policy Guidance

Issuance Date: **September 24, 2008** **Doc. #: PG-08-002**

Subject: **Enterprise Guidance on Operational Risk Management**

To: Office Directors
Chief Executive Officers of Fannie Mae and Freddie Mac

I. PURPOSE AND SCOPE.

A. Risk Management Standards. This Enterprise Guidance on Operational Risk Management (Enterprise Guidance) sets forth standards for the operational risk management programs of the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac) (collectively, the Enterprises), under applicable provisions of the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended by the Housing and Economic Recovery Act of 2008 (HERA), Public Law No. 110-289, 122 Stat. 2654.[1]

B. Evaluation of Risk and Reporting. The examination of operational risk management programs of the Enterprises will be based on the standards set forth herein and include an evaluation of the extent to which internal policies, procedures, activities, and training programs of an Enterprise minimize risk of losses resulting from operational events, as well as the extent to which operational events and operational losses are consistently reported to the agency.

C. Revocation. N/A

II. STATEMENT OF POLICY.

The effective management of operational risk is required to support Enterprise safety and soundness. Each Enterprise must establish a set of policies, procedures, training programs, and other activities which taken together constitute an Operational Risk Management Framework (ORMF) and are reasonably designed to manage its operational risk exposures and comply with regulatory requirements related to operational risk. This

[1] The Federal Housing Finance Agency (FHFA) was established by section 1311(a) of the Federal Housing Enterprises Financial Safety and Soundness Act of 1992 (Safety and Soundness Act or Act) (12 U.S.C. §§ 4501 et seq.), as amended by section 1101 of HERA, Division A, titled the Federal Housing Finance Regulatory Reform Act of 2008 (Regulatory Reform Act). By law, FHFA is to succeed the Office of Federal Housing Enterprise Oversight (OFHEO) in the oversight and supervision of the Enterprises on or before July 29, 2009. In this transition period, the Director of OFHEO serves as the Director of FHFA and oversees the winding up of the affairs of OFHEO (the agency) (See § 1312(b)(5) of the Safety and Soundness Act, as amended).

Enterprise Guidance describes the essential components of an ORMF that should be incorporated into each Enterprise's overall risk management program.

III. REFERENCES.

This Enterprise Guidance sets forth standards pursuant to sections 1311(b), 1313(a) and 1313B of the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended by the Federal Housing Finance Regulatory Reform Act of 2008 (12 U.S.C. §§ 4501 et seq.).

IV. DEFINITIONS.

Director means the Director of OFHEO, or his or her designee.

Operational event means an event characterized by a potential financial loss resulting from inadequate or failed internal processes, people, or systems, or from external events.

Operational loss means a loss (excluding insurance or tax effects) resulting from an operational event.

Operational risk means an exposure to loss from inadequate or failed internal processes, people, and systems, or from external events (including legal risk, but excluding strategic risk).

Operational Risk Management Framework (ORMF) means the set of policies and activities through which a firm manages its operational risk exposures and complies with regulatory requirements related to operational risk.

V. PURPOSE AND INTERPRETATION

A. Strategic Plan and Capital Oversight Plan Requirements

The special examinations of Freddie Mac and Fannie Mae (initiated by OFHEO in 2003 and 2004, respectively) identified serious deficiencies in operational risk management at both Enterprises and highlighted operational risk management as a critical supervisory concern. The Consent Order signed by Fannie Mae in May 2006 and a subsequent supervisory letter to Freddie Mac (June 2006) required each Enterprise to develop plans for operational risk oversight programs and implement them expeditiously. In addition, OFHEO's 2006-2011 Strategic Plan and Capital Oversight Plan (September 2007) both emphasize operational risk management. The Strategic Plan states that OFHEO will develop ways to measure and assess operational risk and apply those measures consistently to both Enterprises. The Capital Oversight Plan states that "OFHEO should encourage, through examination guidance and other actions, the creation of a corporate culture at the Enterprises that embraces management of operational risk." [ii]

B. Supervisory Expectations for Effective Operational Risk Management

In accordance with those objectives, this Enterprise Guidance describes the essential components of an ORMF that should be incorporated into each Enterprise's overall risk management program. The ORMF should establish an operational risk management culture across the Enterprise to identify and address operational risks and a measurement system that quantifies operational risk. The Enterprise should actively use that measurement and quantification to improve operational risk management including the use of this information in an internal economic capital measurement and management program. To meet supervisory expectations for effective risk management, an Enterprise's ORMF must result in tangible benefits to the Enterprise in terms of risk management actions that incent managers to identify and economically manage operational risks.

The Enterprises should focus on meeting the intent and spirit of this Enterprise Guidance rather than whether any specific component is included in an Enterprise ORMF in the exact manner as described herein. Specifically, agency examiners will be instructed to evaluate whether or not the ORMF results in tangible benefits and to document observable results. That examination requirement is referred to herein as a Use Test and is intended to assure that the primary objective of the ORMF is to achieve an effective, rather than merely compliant, operational risk management program.

An Enterprise may recognize similarities between elements of this Enterprise Guidance and the work of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission and of the Basel Committee on Bank Supervision (Basel II). While this Enterprise Guidance draws on those and other sources, it is not the agency's intent to fully adopt either approach. Rather, this guidance reflects agency policy on operational risk management.

The agency recognizes that operational risk is an old, but developing discipline, and that practices, tools, and methods for operational risk management vary and continue to evolve. The agency anticipates that each Enterprise will develop an ORMF with specific features that will evolve over time. The Enterprises will be assessed on the extent to which each respective Enterprise has integrated its ORMF to ensure effective management of operational risk, to provide clear lines of communication and responsibility, and to encourage active self assessment of existing practices and perpetual ORMF enhancements. The agency will promote ongoing internal development efforts by monitoring and evaluating the Enterprise's improvements and plans for prospective developments. The agency encourages on-going dialogue and communications with the

[ii] See id. The Consent Order, supervisory letter, and all applicable provisions in the OFHEO Strategic Plan and Capital Oversight Plan remain in effect for purposes of this Enterprise Guidance pursuant to sections 1301(f) and 1302 of HERA.

Enterprises and will review and revise this guidance periodically as the industry gains experience and operational risk management matures as a discipline.

VI. OPERATIONAL RISK MANAGEMENT

A. Operational Risk Management Framework

An ORMF can be broadly described as the set of policies and activities through which a firm manages its operational risk exposures and complies with regulatory requirements related to operational risk. A successful ORMF 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 firm and consistently applied across all of the firm'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, transferring risk via insurance and other operational risk mitigating strategies.

A critical aspect of the framework is an operational risk capital model. 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 — are 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 firm and its external environment change.

Each Enterprise should ensure that its ORMF is regularly and independently validated and amended to reflect changes in the Enterprise's risk profile and external market developments. The ORMF or any significant changes to an Enterprise's strategies, policies, and procedures for operational risk management should be reviewed and approved by the Board of Directors.

B. Components of the ORMF

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

- Identification and Assessment
- Measurement and Modeling
- Reporting
- Risk Management Decision-Making

1. Operational Risk Identification and Assessment

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

a. Definition of Operational Risk

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

The Enterprise's definition should be reviewed and approved by the Board of Directors. This definition forms the cornerstone of the ORMF in that it determines what diverse group of risks 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 invested. 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 Enterprise should develop processes and mechanisms to assist in identifying operational risks. These should be appropriate for the firm and should include an operational event reporting system and other appropriate management tools such as meaningful key risk indicators and performance triggers, and risk heat maps or scorecards of operational risk exposures. The Enterprise-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 Enterprise 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 Enterprise and should be periodically reviewed and independently validated.

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 control self-assessment process.

2. Measurement and Modeling

Measuring and modeling operational risks are an important part of managing them. 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 should be 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 by the Enterprises for measuring and modeling operational risk should:

- be consistent with a firm-wide definition of operational risk that encompasses the agency's definition as stated above (see footnote 1);
- use valid data derived from an adequate data collection system to support the metrics and assessments of risk;
- be tested for sensitivity to changes in data, assumptions, and model specification; and
- be periodically independently validated.

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

- internal operational event data;
- forward looking business environment assessment;
- internal risk and control assessments;
- external event data; and
- scenario analysis.

The Enterprise's operational risk measurement system should support the calculation and allocation of economic capital for operational risk. The operational risk model should actively incorporate all of the above information sources. 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 relative to others. 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.

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

a. Internal Operational Event and Loss Data

Any internal operational risk measurement system should be supported by event and loss data derived from the operational event tracking system described above. This database should be established as soon as feasible and eventually include operational event and loss data covering five or more years. It is recognized that data may become stale for some uses. For example, past losses may no longer be indicative of potential future losses when new controls or changes in business strategies make particular loss events much less likely to occur. However, data should not be discarded since it remains relevant for other uses such as scenario analysis, regulatory compliance reporting, and "lessons learned" material 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. Instructions for Operational Event Data Collection and Reporting

For purposes of operational risk management and measurement the Enterprises should track the incidence of and losses related to operational events. The agency's expectations regarding systems for collection and reporting of internal operational events and losses are contained in a letter to the Enterprises, *Instructions for Operational Event Data Collection and Reporting*. The Instructions include regulatory reporting instructions and requirements for an operational event and loss data collection and reporting system.

For operational risk management purposes, the agency 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 consequences of operational events. However, operational losses do not include costs related to risk management and enhancements to controls, systems, and processes to prevent future operational losses.

The agency recognizes that accurately calculating certain losses from operational events can be difficult, particularly for 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, the agency expects those losses to be considered in the ORMF.

c. Business Environment Assessment

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

d. Internal Risk and Control Environment Assessment

The Enterprise's operational risk measurement system should have a component that takes into account the condition of its internal control environment. The Enterprise 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 Enterprise'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. Adjustment factors can be incorporated into the Enterprise' quantification methodology in different ways and, while not prescribing a specific methodology, the agency will assess the processes used by the Enterprises to integrate qualitative and quantitative measures of the internal control environment factors into the quantification of operational risk exposure.

e. External Loss Data and Scenario Analysis

Scenario analysis and external data on industry operational loss events can be important tools of an effective ORMF, if carefully designed and integrated into the processes and systems for risk measurement and management. The Enterprise'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 Enterprise'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 Enterprise'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. The Enterprise should have a process for incorporating scenario analysis into its operational risk measurement system. The Enterprise 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 loss events they are intended to reflect; and the results of the analysis and how these results impact operational risk measurement.

f. Review and Validation

A timely review and update of an Enterprise's operational risk measurement system is justified whenever the Enterprise becomes aware of information that may have a material effect on the estimate of operational risk and operational risk capital allocation. A complete review of the Enterprise'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.

3. Reporting

a. Regular Reporting Structure

The entire ORMF 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 Enterprises 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 Enterprise.

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:

- Significant operational loss events in the prior quarter, including near misses;
- Material changes in factors signaling any increased or decreased risk of future losses;
- Significant changes in the state of the Enterprise's processes and resources, with comparison to the previous report using specific indicators or metrics; and
- Policy and risk tolerance reporting.

4. Risk Management Decision-Making

Effective operational risk management goes beyond implementing effective controls and requires positive decision-making to manage the risks an Enterprise is taking. Operational risk should be addressed through effective techniques of avoidance, transfer, mitigation, and appropriate monitoring and resource allocation for explicitly accepted risks. Controls throughout the Enterprise should meet industry standards, and examiners will be instructed to evaluate the effectiveness of mitigation measures, both in terms of control-oriented approaches to prevent the occurrence of events and traditional insurance programs to limit the severity of events that do 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. No matter which decision framework is chosen, the decision framework should be applied consistently across the Enterprise. Consistent 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 and investments consistent with each other and the Enterprise's risk policies.

The agency may review Enterprise allocations of economic capital for managing operational risk. Such review 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 Enterprise.

C. Operational Risk Governance: Management Responsibilities and Duties

The ORMF should define the roles and responsibilities of key players and of corporate-wide functions. Key players include senior management and the Board of Directors, a chief risk officer, a risk oversight committee, business unit managers, and individuals from typical 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 ORMF and its relationship with other areas of management, in particular how senior the highest operational risk management officer is in the firm and the lines of communication to more senior management and the Board of Directors. 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 must support the effective implementation of the ORMF. 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 incentive structure should be reinforced through performance assessments (and, consequently, manager compensation) that reflect achievement of the ORMF objectives, including appropriate capital allocations.

Each level of governance has certain roles and responsibilities within the ORMF. Agency supervision staff will assess whether an Enterprise has assigned and executed responsibilities for ORMF that are equivalent to, or achieve the same desired outcome as, those described below.

1. Board of Directors

The Board of Directors is responsible for approving the ORMF and ensuring that adequate resources are available to accomplish the task of managing operational risk. The Board should be aware of and understand the sources of operational risk for the Enterprise and the strategy to be employed to address that risk. Specific responsibilities of the Board relate to:

a. Risk Management Function.

The Board should approve the establishment of a firm-wide independent operational risk management function within the Enterprise that will be responsible for the day-to-day implementation of the ORMF.

b. Policy.

The Board should review and approve the implementation of an ORMF and any major changes to it. It should review and approve the policy provisions that establish the major framework elements and management's plans to implement the ORMF, including identifying and assessing, measuring, monitoring, and managing risk. While management's role is to ensure that procedures implementing the ORMF are developed and are effective, the Board must be given sufficient information to understand and approve the ORMF and any significant changes to it.

c. Validation.

The Board should ensure that the ORMF is validated by a qualified independent team of experts, staffed either externally or internally.

d. Resource Allocation.

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

e. Compensation Programs.

The Board should ensure that the effectiveness of the Enterprise's operational risk management is reflected in the performance evaluation and compensation of senior management.

2. Senior Management

Senior management should be actively involved in ensuring that the ORMF is consistently applied across the Enterprise. Specifically, senior management has the following areas of responsibility:

a. Culture.

In order for the ORMF to be effective, senior management should set an appropriate tone and ensure that all levels of staff clearly understand their roles and responsibilities for operational risk management within the Enterprise, the sources of operational risk, and the Enterprises' operational risk management strategies.

b. Allocation of Resources.

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

c. ORMF Oversight.

Senior management should annually review and update as appropriate the ORMF and related policies that are approved by the Board. In addition, senior management should review reports on operational events, risk and control assessments, and risk measurements to assess effectiveness of the operational risk management function.

3. Operational Risk Officer

An independent firm-wide operational risk officer appointed by senior management or the Board of Directors should be responsible for the day-to-day implementation of the ORMF. This individual 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; codifying policies and procedures for operational risk management; designing and implementing the Enterprise's operational risk assessment methodology; designing and implementing the operational event data collection and reporting system; and overseeing the operation, maintenance, and improvement of the components of the ORMF once they have been established.

a. 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.

b. 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 the agency's reporting requirements.

c. Operational Risk Economic Capital.

The operational risk officer should have responsibility for establishing an analytic framework that supports the calculation and allocation of economic capital for operational risk. The operational risk officer should work with Enterprise senior management to ensure that the allocation of operational risk capital is consistent and supportive of effective risk management. Operational risk of the Enterprise should be calculated on a periodic basis and reported to business unit managers, senior management, and the Board of Directors.

d. Documentation of Policies and Procedures.

The operational risk officer is responsible for maintaining documentation of policies and procedures for the ORMF. 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 Enterprise'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 Enterprise should document its process for the self-assessment of operational risk and internal controls by business units.

e. 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.

4. Business Line and Administrative Unit Management

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

- reflects risk taking, risk management decisions, and operational risk controls consistent with the Enterprise's risk appetite as approved by the Board of Directors;
- safeguards resources;
- produces reliable management reports;
- complies with applicable laws and regulations; and
- minimizes the potential for human error and fraud.

Business line and administrative unit management should periodically self-assess the use of ORMF 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.

5. Independent Verification and Validation of the ORMF

An effective ORMF should include independent verification and validation. The Enterprises may use independent and qualified internal or external parties to perform verification and validation. The scope of such reviews should be sufficient to assess the effectiveness of the ORMF 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.

D. Use Test

The Enterprise will be subject to a supervisory review that must include the application of a Use Test to the ORMF of the Enterprise. The Use Test seeks to confirm that the ORMF conforms to the following principles:

- It is not limited to satisfying this guidance and/or other regulatory requirements;
- It evolves as the institution gains experience with operational risk management strategies and results; and
- It provides tangible and, where possible, measurable benefits to the organization in the management and control of risk.

Evidence that the operational risk framework of the Enterprise meets this Use Test may include documented linkages between the various parts of the framework (risk identification and assessment, measurement, and reporting) and management decision making. For example, the operational risk framework 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. Evidence that these processes are more than a compliance exercise, are effectively implemented and elicit the appropriate management response will be required to pass the Use Test.

For purposes of supporting a Use Test review, the Enterprise will be required to produce evidence that the operational risk event collection, reporting, and measurement systems are periodically reviewed and updated with appropriate adaptations to changes in the internal control environment and external business and regulatory context. For example, evidence to satisfy the Use Test could be internal written communications that demonstrate that management at the Enterprise takes into account the results of the operational risk measurement and reporting systems when making business decisions.

The Use Test review will also assess the extent to which the Enterprise can 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 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.

VII. REPORTING PROCEDURES AND ADDITIONAL MATTERS.

A. Submission of Operational Risk Framework Plans to the Agency

As a matter of effective ongoing communication with the agency and to enable the agency to properly assess the adequacy and effectiveness of the ORMF and processes, the Enterprise should submit plans for implementing an operational risk management framework to the agency. The Enterprise should inform the agency in a timely fashion of any material alterations to the plan or implementation timeline. When practical and appropriate, interim written updates to the plan are recommended.

B. No waiver of privilege.

An Enterprise does not waive any privilege it may claim under law by submitting any report or information required under this Guidance.

C. Supervisory Action.

Failure to comply with this Enterprise Guidance may subject the Enterprise or members of the Board of Directors, officers, or employees thereof to supervisory action by the agency under the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended, including but not limited to, cease-and-desist proceedings, civil money penalties, and removal or suspension from participation in the conduct of the affairs of an Enterprise.

D. Retention of records.

An Enterprise must retain copies of any plan or report submitted to the agency under this Enterprise Guidance and all original supporting documentation or business record equivalent in a central location for a period of not less than five (5) years from the date of submission. All supporting documentation must be provided to the agency or other governmental or law enforcement authorities upon request.

E. Preservation of existing authority.

Nothing in this Enterprise Guidance in any way limits the authority of the agency to otherwise address unsafe or unsound conditions or practices or violations of applicable law, regulation, or supervisory order. Action referencing the Enterprise Guidance may be taken in separate form, in conjunction with, or in addition to any other supervisory or enforcement action available to the agency under law. Compliance with the Enterprise Guidance in general would not preclude a finding by the agency that an Enterprise is otherwise engaged in a specific unsafe or unsound practice or is in an unsafe or unsound condition, or preclude the agency from requiring corrective or remedial action with regard to such practice or condition. That is, supervisory action is not precluded against an Enterprise that has not been cited for a deficiency under this Guidance. Conversely, an Enterprise's failure to comply with one of the requirements set forth in the Enterprise Guidance may not warrant a formal supervisory response from the agency, if the agency determines that the matter may be otherwise addressed in a satisfactory manner. For example, the agency may require the submission of a plan to achieve compliance with the particular requirement or standard.