Table of Contents

Introduction

This Federal Housing Finance Agency (FHFA) module for *Enterprise Risk Management* (ERM) is designed as a resource and reference for all FHFA examiners. The module contains fundamental information and procedures intended for the examination of the Federal National Mortgage Association (Fannie Mae), the Federal Home Loan Mortgage Corporation (Freddie Mac), the Federal Home Loan Banks (FHLBanks), and the FHLBanks' Office of Finance (OF). References to the regulated entities[1] in this module also apply to the OF (unless otherwise noted). Collectively, these institutions will be referred to as the "regulated entities" and individually as a "regulated entity." Fannie Mae and Freddie Mac may also be referred to collectively as the "Enterprises" or individually as an "Enterprise." The module contains a workprogram with a broad range of worksteps within five categories, and examiners should identify and perform those worksteps most relevant to reach conclusions given the scope of the examination.

Managing risk across a regulated entity is an essential element of its overall risk governance. An institution-wide risk management approach considers the extent to which risks overlap or are interrelated. It also encompasses all on- and off-balance sheet risks at entity-wide, portfolio, and business-line levels. The primary objectives of an ERM program are to identify, measure, monitor, and report on the individual and aggregate levels of risks and the trends of risk exposures in relation to an institution's established risk limits and risk appetite. An ERM program includes policies and procedures to carry out risk management objectives across the entire institution.

The Committee of Sponsoring Organizations of the Treadway Commission asserts that an institution that integrates sound risk management practices throughout the entity can realize benefits including but not limited to:

- Identifying and managing risk institution-wide to sustain and improve performance;
- Reducing performance variability by anticipating risks that could affect performance and taking actions to minimize disruption and maximize opportunity;

[1] The OF is not a "regulated entity" as the term is defined at 12 USC 4502(12). However, for convenience, references to the "regulated entities" in this module should be read to apply also to the OF.

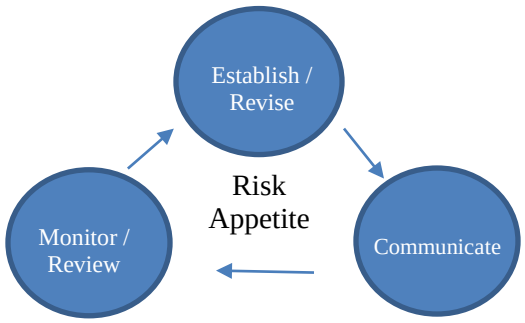
- Increasing positive outcomes and reducing negative surprises and costs by improving an institution's ability to identify risk and establish appropriate responses;
- Enhancing institutional resilience by anticipating and responding to change, not only to survive but to evolve and thrive;
- Increasing the range of opportunities by considering both positive and negative aspects of risk to identify new opportunities and unique challenges with current opportunities; and
- Improving resource deployment by obtaining robust information on risk to assess overall resource needs.

Background

FHFA's regulation, *Responsibilities of Boards of Directors, Corporate Practices, and Corporate Governance Matters* 12 CFR Section 1239.11 (Rule), requires each regulated entity to have in effect at all times an ERM program that incorporates the regulated entity's risk appetite, aligns the risk appetite with the regulated entity's strategies and objectives, addresses the regulated entity's exposure to credit risk, market risk, liquidity risk, business risk, and operational risk, and complies with the requirements of the Rule and with all other applicable FHFA regulations and policies.

The Rule also requires that the board of directors approve the ERM program that establishes the regulated entity's risk appetite. The risk appetite describes the aggregate level and types of risk the board of directors and management are willing to assume to achieve the regulated entity's strategic objectives and business plan, consistent with applicable capital, liquidity, and other regulatory requirements. Not all risks pose the same potential harm – whether financial, reputational, or operational – to a regulated entity. Therefore, the board of directors or board risk committee should consider the regulated entity's risk capacity during its review of the regulated entity's risk appetite.

As illustrated below, the risk appetite is established, then communicated throughout the regulated entity, monitored, reviewed periodically, and revised as needed.



As required by the Rule, the ERM program must include: appropriate risk limits for business lines; policies and procedures relating to risk management governance; risk oversight infrastructure; processes and systems for identifying and reporting current and emerging risks; and provisions for monitoring compliance with risk limits and policies relating to risk management governance, risk oversight, and effective and timely implementation of corrective action. Further, the ERM program must:

- Include provisions specifying management's authority and independence to carry out risk management responsibilities; and
- Integrate risk management with management's goals and compensation structure.

Risk limits and metrics must be consistent with the activities and objectives of business units and functional areas. Ideally, risk limits are expressed so they can be:

- Consistent with the capital, liquidity, or other risk metrics used to define objectives;
- Applied to strategic and operational objectives; and
- Implemented by business lines through policies and procedures across the institution.

Risk limits may be expressed through outcome measures of key objectives. For example, as part of interest rate risk management, a regulated entity might set a daily target of zero for its balance sheet duration gap, but accept outcomes of +/- two months. Given this risk limit, a duration gap in excess of +/- two months would be reported as a breach. Resolution of breaches or mitigation of emerging risks should be addressed through documented action plans for specific risks and groups of risks.

In an ERM program, each business unit or functional area is considered the owner of its risks. Accordingly, each should have policies and processes in place to ensure adherence to all applicable risk limits and risk management governance requirements. These policies and processes should allow the business unit or functional area to appropriately identify, assess, document, and report current and emerging risks. For risk-taking business units, the processes should include formal risk-based self-assessments with common terminology and consistent time horizons used across the regulated entity. In addition, business units and functional areas should analyze any breaches of risk limits or exceptions to risk management governance requirements and identify the root cause(s) of any such breaches or exceptions.

The Rule does not require a particular structure for the ERM function. Staff performing the ERM function should possess sufficient qualifications and experience to fulfill their roles. A regulated entity may carry out the ERM function with: staff in a dedicated ERM unit; staff embedded within business units (but reporting outside the business unit); or staff in both a dedicated unit and embedded within business units. Although staff performing the ERM function often works closely with business unit personnel, they must distinguish between assisting business units with risk analyses and making risk decisions to maintain independence. They should have the expertise to critically review and, when appropriate, challenge business practices that may result in inappropriate risk to the institution.

The Rule does specify the responsibilities of the enterprise risk management function to include:

- Allocating risk limits and monitoring compliance with such limits;
- Establishing appropriate policies and procedures relating to risk management governance, practices, and risk controls, and developing appropriate processes and systems for identifying and reporting risks, including emerging risks;
- Monitoring the level and trend of risk exposures, including testing risk controls and verifying risk measures; and
- Communicating within the organization relevant risk management issues and/or emerging risks, and ensuring that risk management issues are effectively resolved in a timely manner.

To promote a consistent risk culture across the regulated entity, common language should be used to identify and define current and emerging risks, and risks should be measured and monitored in a uniform manner, from both business unit and enterprise-wide perspectives. The process for assessing key risks at all levels of the institution and across

all business units or functional areas should be standardized, to the extent possible, and sufficiently responsive to changing conditions affecting the institution's risk profile.

The ERM function should include reporting processes that ensure the ERM staff receives the data required to conduct its risk monitoring responsibilities and document its performance. This performance documentation also allows the ERM function to be independently reviewed.

In addition, the ERM function should have a documented business recovery plan which is reviewed regularly. Stress tests should also be conducted to assess the reasonableness of key assumptions in the recovery plan. If modeling is used as part of other risk identification and assessment processes, the ERM staff should also confirm the reasonableness of those key assumptions. In addition, ERM staff should solicit feedback regarding the business unit's perception of the effectiveness of the risk management activities.

In a "three lines of defense" structure, the risk management staff with responsibilities for oversight and effective challenge to the risk-taking units and functional areas is frequently described as the "second line of defense." The risk-taking business units that are accountable for identifying and addressing risks in their businesses and for operating a sound control environment are the "first line" of defense; internal audit, which is independent of both the business units and the ERM function, may also test and evaluate the risk governance structure, risk management activities, and the internal control processes as the "third line" of defense.

The head of the ERM function is the chief risk officer (CRO), according to the Rule. The CRO implements and maintains appropriate ERM practices for the regulated entity, and reports directly to the board's risk committee and to the chief executive officer (CEO). The CRO should have stature and risk management expertise that is commensurate with the regulated entity's capital structure, risk appetite, complexity, activities, size, and other appropriate risk-related factors. The CRO's performance evaluation and compensation should be structured to provide for an objective and independent assessment of the risks taken by the regulated entity.

The CRO must report regularly to the board risk committee and the CEO. Per the Rule, the CRO's reports must address: significant risk exposures and related controls, changes to the risk profile, risk management strategies, results of risk management assessments or reviews, and emerging risks. The CRO must also report regularly on the regulated entity's compliance with, and the adequacy of current risk management policies and procedures, and recommend any adjustments to such policies and procedures that the

CRO considers necessary or appropriate. These reports might include, for example, information about: concentration risk, correlation of risks, or aggregate risk relative to the risk appetite and the comprehensiveness of business unit risk assessments. CRO reports may also address:

- The magnitude, frequency, and recurrence of any breaches of risk limits;
- Recommendations made in response to any breaches of risk limits;
- Any failures of business units to adhere to the policies and procedures within the ERM program;
- Management's responses to, and the consequences of any such failures; and
- The results of stress tests under a range of possible scenarios and assumptions.

CRO reports should also contain information on the level and trend of the regulated entity's risk exposures. The CRO should have the ability to meet with the board or board risk committee without the CEO or other management present to allow for open dialogue.

Applicability of this Module to the Office of Finance (OF)

Examiners should apply this module when examining the OF, notwithstanding that the risk management requirements of the Rule apply directly only to the regulated entities. Applying risk principles to the OF is consistent with FHFA's oversight authority regarding the OF, as well as with other provisions of the applicable statutes and regulations.

The term "regulated entity" is defined by statute at 12 USC 4502(20), to include only Fannie Mae, Freddie Mac, and the FHLBanks. Although the OF is not a regulated entity, the Safety and Soundness Act separately gives the FHFA Director general regulatory authority over the OF, including the broad power to "to ensure that the purposes of the Safety and Soundness Act, the Federal Home Loan Bank Act, and any other applicable law are carried out" (*Establishment of the Federal Housing Finance Agency* (12 USC 4511(b)(2)). The FHFA Director also has the statutory duty to ensure that each regulated entity operates in a safe and sound manner (*Duties and authorities of the Director* (12 USC 4513(a)(1)(B)(i))).

The OF's principal activity is to issue and service the consolidated debt obligations that finance the FHLBanks' business activities. The OF functions as the gateway between the FHLBanks and global capital markets, a role that is fundamental to the operations of the FHLBanks. If the OF does not prudently manage the risks associated with those operations, its failure to do so could adversely affect the safety and soundness of the

FHLBanks and their ability to carry out their statutory mission. Accordingly, FHFA examines the OF's operations, including its risk management practices, pursuant to its general regulatory authority over the OF, as well through its authority to ensure that the FHLBanks remain able to operate in a safe and sound manner, which includes having efficient and reliable access to the capital markets.

Including the OF is consistent with other provisions of the Safety and Soundness Act, one of which includes the OF within the definition of an "entity-affiliated party" (12 USC 4502(11)). The effect of that definition is to authorize FHFA to initiate administrative enforcement actions, such as a cease-and-desist action, against the OF, if necessary to address any unsafe or unsound practices relating to the business of the OF (*Cease-and-desist proceedings* (12 USC 4631(a)(1))). That would include the authority to initiate such an action if the Director believed that the OF's risk management practices were deficient. In addition, the regulations under which the OF operates require that the OF board of directors establish policies that, among other things, require that the consolidated obligations be issued efficiently and at the lowest all-in cost, consistent with "prudent risk management practices" (*Office of Finance* 12 CFR 1273.6(d)(4)). FHFA's general regulatory authority over the OF also allows FHFA to examine the risk management practices related to the issuance of the consolidated obligations to ensure compliance with this regulation.

Regulatory Environment

The primary regulations, supervisory guidance, and other resources applicable to the regulated entities' ERM activities are listed below. Other resources that may be helpful to examiners are also listed.

Rules and Regulations relevant to ERM

- FHFA, Responsibilities of Boards of Directors, Corporate Practices, and Corporate Governance Matters (12 CFR Part 1239)

- FHFA, Prudential Management and Operations Standards, Standard 1: Internal Controls and Information Systems (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 2: Independence and Adequacy of Internal Audit Systems (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 3: Management of Market Risk Exposure (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 4: Management of Market Risk – Measurement Systems, Risk Limits, Stress Testing, and Monitoring and Reporting (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 5: Adequacy and Maintenance of Liquidity and Reserves (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 6: Management of Asset and Investment Portfolio Growth (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 7: Investments and Acquisitions of Assets (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 8: Overall Risk Management Processes (Appendix to 12 CFR Part 1236)

- FHFA, Prudential Management and Operations Standards, Standard 9: Management of Credit and Counterparty Risk (Appendix to 12 CFR Part 1236)

FHFA Examination Resources relevant to ERM

FHFA Advisory Bulletins

- AB-2017-02: Information Security Risk Management (09/28/17)

- AB-2017-01: Classifications of Adverse Examination Findings (03/13/17)

- AB-2016-05: Internal Audit Governance and Function (10/07/16)

- AB-2015-07: Fraud Risk Management (09/29/15)

- AB-2014-02: Operational Risk Management (02/18/14)

- AB-2013-07: Model Risk Management Guidance (11/20/13)

- AB-2013-01: Contingency Planning for High-Risk or High-Volume Counterparties (04/01/13)

- AB-2005-05: Risk Management Oversight (05/18/05)

FHFA Examination Manual

- Board of Directors and Senior Management (07/13)

- Strategic Planning (03/13)

Non-FHFA Examination Resources relevant to ERM

- Bank for International Settlements, Basel Committee on Banking Supervision (Basel Committee): Principles for effective risk data aggregation and risk reporting (2013)

- Financial Stability Board, Senior Supervisors Group: Risk Management Lessons from the Global Banking Crisis of 2008 (2009)

- Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management – Integrating with Strategy and Performance (2017)

- Office of the Comptroller of the Currency, Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations (12 CFR Parts 30, 168, and 170)

Examination Workprogram

The workprogram for the examination of *Enterprise Risk Management* is detailed below. Examiners are expected to develop procedures that satisfy the specific objectives of the examination activity. The procedures should support the examination work program and, when executed, provide sufficient evidence to support a conclusion regarding the objective. Examiners should not exclusively rely upon representations made by management or work performed by other internal or external parties to support conclusions regarding an examination objective.

Examination procedures should include testing designed to confirm that policies, procedures, controls, or models operate as intended. This may be achieved through transaction testing or other testing methods. In limited circumstances, examiners may determine that testing cannot be reasonably conducted. Examples of such circumstances include cases where there is insufficient data, a program or product is too new to test, or when testing cannot be scaled to a manageable level. In these instances, examiners are expected to document in the examination procedures, with the examination manager's approval, the rationale for not conducting testing.

An examiner may leverage testing performed by internal and external parties, such as internal or external audit functions, if (i) the testing used to support the examiner's conclusions is clearly applicable in the scope of the examination activity, and (ii) the examiner has assessed the methodology and results of any testing that is used to support the examiner's conclusions.

NOTE: *Text in italics referenced in a work step represents illustrative guidance that serves as suggestions for specific inquiry.*

1. Scope of Examination Work Performed

1) Review workpapers from the most recent examination when the scope included a review of ERM.

2) Assess the status or review the remediation progress based on management's commitments of any outstanding examination findings (*e.g.*, Matters Requiring Attention, Violations or Recommendations) pertaining to ERM.

3) Review internal audit or quality assurance reports for outstanding issues relating to ERM.

4) Review [for and address] any applicable portions of FHFA issued Advisory Bulletins or other examination guidance.

5) For Enterprise examinations, access the DOC Status Tracking and Reporting (DOC STAR) system to determine whether decisions (*e.g.*, Directives, Orders) by the Conservator impact the scope of the examination work.

6) Review minutes of meetings of the board of directors and relevant board and senior management risk and compliance management committees for the previous twelve months for any issues regarding ERM.

7) Evaluate the adequacy of the scope and testing completed or validated by ERM staff and determine the status of corrective actions for findings. *(Does ERM staff evaluate risks across the business units, including aggregate and concentration risks?)*

Summarize the work performed in the *Enterprise Risk Management* workprogram. To the extent there were modifications to the originally planned scope based on concerns identified during the examination, document those changes and the reasons for such changes.

2. Description of Risks

Examiners should develop an understanding of the ERM program at the regulated entity. This information may be obtained through a review of current and historic regulated entity risk assessments or other risk-related reports.

1) In determining the existence of risks related to ERM at the regulated entity, consider possible deficiencies or sources of risk from the following:

   a) Inappropriate risk appetite statement;

   b) Inadequate policies and procedures comprising the ERM program;

   c) Inappropriate risk limits or measures;

   d) Inadequate reporting systems that fail to identify limit breaches, concentrations, or emerging risks;

   e) Inadequate breadth of scenarios used in stress testing; and

f) Inappropriate delegation of risk monitoring from ERM staff to business unit personnel.

2) Determine whether enterprise-wide risks are included and quantified in risk assessments or other risk-related reports and whether trends are identified.

3. Risk Management

Risk Identification Process

1) Based on work steps performed under **Description of Risks,** consider the adequacy of the regulated entity's risk identification process with respect to ERM and impacted business activities.

2) Determine whether the regulated entity has established an appropriate risk culture and ERM program such that business unit senior management has taken appropriate action to identify, assess, and report current, and emerging risks that could affect the achievement of the regulated entity's strategies, goals, and objectives. Consider whether:

   a) Business units identify risks based on both potential events and the current operating environment;

   b) Risk-based self-assessments are a formal and ongoing process throughout the institution, and if management across the institution uses common terminology and time horizons; and

   c) The process for assessing key risks at all levels of the institution and across all businesses is consistent, standardized, and sufficiently responsive (in order to respond to changing conditions).

3) Assess the effectiveness of the identification, design, and development of actions that will best address risks and ensure business activities are consistent with the regulated entity's ERM program (*e.g.*, risk avoidance, mitigation, or acceptance). Consider whether:

   a) Business unit management develops action plans for specific risks and groups of risks;

b) Key risk strategies are communicated to and approved by appropriate management levels;

c) Risks are able to be appropriately measured, monitored, and reported by ERM staff; and

d) ERM staff verifies data sources utilized by the business units for their risk assessments. *(Are action plans for specific risks documented and appropriate? Has ERM staff documented its verification of data sources?)*

4) Review and evaluate the regulated entity's method for aggregating risks to develop a portfolio view of risk across the institution. Consider whether:

a) The risk assessment process considers risks from both a business unit and entity-wide perspective;

b) ERM staff evaluates whether the institution's aggregated risk profile is consistent with the institution's board-approved risk appetite;

c) ERM staff performs adequate analyses to be used by the board of directors in assessing the institution's risks; and

d) ERM staff considers the correlations among risks when evaluating and monitoring risks and action plans. *(Does ERM staff employ both qualitative and quantitative techniques appropriately? Does ERM staff utilize modeling techniques? If so, are assumptions reasonable and conclusions supported? If risk modeling is performed by business units, does ERM staff approve assumptions and validate the processes?)*

5) Evaluate the self-assessment process and how ERM staff uses risk-based self-assessments to assess and implement the ERM program. Consider the following:

a) Timing and frequency;

b) Consistency of measures and analytical approaches, including terminology and time horizons;

c) Evidence of effectiveness; and

d) Determine if any action was taken as a result of the assessments and the status of any corrective actions. (*If limit breaches occurred, did the self-assessment for that function identify the potential for such a breach?)*

6) Verify that new products and services are captured in the risk assessment process and that ERM staff participates in the approval process for new business activities. *(Are ERM staff members included in the new product or services approval process?)*

Organizational Structure

1) Review the organizational structure and determine if the CRO reports directly to the board of directors, and/or a risk management committee of the board, and the CEO. Determine whether the CRO has direct access to all levels of management, staff, and the board or board risk committee. *(Does the CRO report directly to the board or board risk management committee? Does the CRO have appropriate access to the board, board committees, and CEO to provide for effective challenge? Is the CRO sufficiently independent of influences from the risk-taking functions? Does the risk management function inappropriately include risk-taking activities?)*

2) Identify any ERM staff who also have reporting lines to or from business unit personnel. (*Why is there dual reporting? What steps have been taken to ensure the ERM staff's independence?)*

3) Determine and assess the independence of ERM staff who work closely with business line personnel. Consider the following:

   a) Performance evaluation process; and

   b) Compensation and/or bonus goals. *(Do business unit managers have input to the performance evaluation or compensation of ERM staff?)*

4) Determine how decisions related to the ERM program are made and responsibilities assigned. (*Are decisions related to the ERM program consistent with the formal delegations of authority?*)

   a) Determine if the board of directors or the board risk management committee requires and receives regular updates on aggregate and key business unit risks *(Do minutes of the risk committee and attachments contain adequate information about aggregate and key risks?*);

b) Assess the appropriateness of the ERM function's structural organization and delegations of authority;

c) Assess the timeliness of the information the board of directors receives on changing risk profiles, including new, additional, or emerging risks; and

d) Assess ERM's human capital and funding resources. Determine if ERM staff have the education, experience, training, and professional certifications to perform their duties and responsibilities effectively. *(Does the ERM staff have sufficient product knowledge? Are the skills of ERM staff aligned with current and emerging risks? Is there a program of continuing education for ERM staff?)*

5) Determine the extent to which risk identification, monitoring, and remediation are factored into management performance evaluations.

6) Determine how ERM staff maintains contact with business units or operational functions. Consider the following:

a) Whether the CRO or other senior ERM staff participate in any senior management risk committee meetings;

b) How the ERM staff use business unit self-assessments, and if ERM staff assess whether the conclusions, recommendations, and assigned ratings from these assessments are accurately portrayed in an annual entity-wide risk-based self-assessment report;

c) Whether ERM staff are directly placed with business units or with functional areas reporting to the CRO;

d) The existence of business-line or functional unit personnel with indirect reporting lines to the CRO; and

e) The existence of an independent review process within the risk management function that conducts periodic, or continuous, assessments of business-line or functional unit activities.

Policy and Procedure Development

1) Evaluate the appropriateness of ERM policies in consideration of:

   a) Whether policies for individual business units are consistent with ERM policies;

   b) Whether policies include guidance, either explicit or by reference, to procedures on managing and identifying risk and responsibility for establishing risk limits;

   c) Whether polices related to specific risk areas (*e.g.*, credit risk, market risk, liquidity risk, business, and operational risk) are communicated and enforced across the regulated entity;

   d) Whether risk metrics are appropriate; and

   e) Whether ERM policies are periodically reviewed to ensure alignment with the board-approved risk appetite.

2) Determine if there are established communication channels among the ERM staff, the board of directors, senior management, and the business units regarding key risk information and risk management processes. *(Is information regarding risks communicated appropriately throughout the institution?)*

3) Assess the communication between ERM staff and the board of directors, or board risk management committee, that address the following subjects:

   a) Adequacy of and compliance with the institution's risk management policies and procedures and suggested changes to risk management policies and procedures;

   b) Risk appetite and risk limits, including the ERM staff's judgment of the reasonableness of the limits and the consistency of the application of those limits across all business units;

   c) Management-approved exceptions to risk limits and the ERM staff's judgment concerning those exceptions, including assessment of justification and documentation;

   d) Instances of the CEO not adhering to, or holding business units accountable for adhering to the ERM program; and

e) Risk-limit breaches and the ERM staff's judgment regarding the identification, impact severity, resolution, and reporting of those breaches. *(Are root cause analyses performed? Are risk limit breaches evaluated for recurrence, severity, and impact on the institution?)*

4) Assess the adequacy of the institution's risk analysis and risk measurement tools and techniques. Consider whether:

   a) Qualitative approaches are used, where appropriate, to measure the effect of risk given different scenarios;

   b) Risk owners evaluate and provide ERM staff with feedback on the effectiveness of the risk management activities;

   c) Risk assessment measurements are aligned with the institution's risk appetite and liquidity, capital, or other risk metrics; and

   d) The risk assessment process stress tests the key assumptions of risk models.

5) Review and evaluate the institution's integration of risk management activities into decision-making processes. Consider whether management decisions are based upon limits, risk appetite, and potential effects of risks on strategies, goals, and objectives.

6) Evaluate how ERM staff uses the business unit risk-based self-assessments.

7) Assess the effectiveness of actions taken by management to correct deficiencies in risk management practices. *(Are corrective actions completed in a timely manner and reported to the board?)*

Risk Metrics

1) Review and evaluate the process for establishing and communicating the regulated entity's risk appetite and individual risk limits. Consider the following:

   a) Processes for establishing liquidity, credit, or other risk limits;

   b) Scope and thoroughness of risk evaluations; and

   c) Clarity, timeliness, and completeness of risk reporting to the board of directors.

(Are the risk limits appropriately comprehensive? Is the CRO's risk assessment consistent with the business units' risk assessments? If not, have the differences been satisfactorily explained?)

2) Evaluate management's efforts to establish controls, and implement risk mitigation activities. *(Are risk limits and controls consistent with the risk appetite established by the board?)*

Reporting

1) Assess the ERM function's review of the risk reporting practices of the business units and operational functions. Consider both internal documentation practices and reporting to senior management and the board or board risk management committee.

2) Review and evaluate the quality and frequency of CRO reports presented to the board of directors or the board risk management committee. Consider whether:

   a) The board of directors or board risk management committee monitors key risks using specific liquidity, credit, or other risk metrics and standardized reports that evaluate the effectiveness of the institution's risk management strategies, actions, and processes;

   b) Aggregate risks and risk correlations are measured and reported;

   c) Emerging risks and breaches of risk limits are reported on a timely basis by both ERM staff and the business unit, and include the ERM staff's assessment of frequency, severity, and impact on the institution; and

   d) Resolution (or proposed resolution) of risk limit breaches was appropriate and reported on a timely basis.

3) Review the minutes of the board of directors and the relevant board risk management committee meetings to determine if the information reported by ERM staff is sufficient for the board of directors to fulfill its oversight obligations and that the information provided to the board of directors is timely, accurate, consistent, and relevant.

Internal/External Audit

1) Determine whether the internal audit function regularly evaluates the ERM function and established risk management processes.

2) For internal audits completed on the ERM function since the previous examination, consult with the Office of the Chief Accountant (OCA) regarding any findings about the adequacy of the scope and testing performed by internal audit.

3) If there are no prior findings, select internal audits related to ERM and determine whether or not the scope of the audit was adequate and assess the adequacy of workpapers to support findings. (*Does the scope include an assessment of internal policies and procedures? Does the scope include testing of operational processes? Do the workpapers include a clear trail to conclusions? Do the workpapers identify areas for further review?)*

4) Coordinate with OCA to determine whether or not the external auditor performed work related to ERM processes and whether or not OCA performed an evaluation of the adequacy of the scope and any testing completed by the external auditor.

Information Technology

1) Identify and assess the automated and manual systems and applicable controls for processing and supporting ERM. (*Are authorities and responsibilities clearly defined? Are delegations current? Do information systems provide the information needed to make informed and timely decisions? Are authorized change processes followed as data is acquired from sub-systems?)*

2) Determine if the regulated entity has developed and tested a business continuity plan for ERM-related areas. (*Are systems specific to ERM considered in the business continuity plan? Does the regulated entity or have appropriate contingency procedures to ensure ERM processes would continue to operate despite unexpected interruptions?)*

Compliance

1) Evaluate if the regulated entity has appropriate policies and procedures to confirm compliance with applicable laws, rules, regulations, and internal controls. *(What was the underlying cause for any violation or non-adherence? Were proper procedures followed in the event of non-adherence? Has the regulated entity strengthened*

internal controls to prevent recurrence?)

4. Testing

1) Select a sample of recently completed ERM staff evaluations of business unit risk-based self-assessments and evaluate the adequacy, consistency, and timing of the assessments. *(Do the risk assessments identify major and emerging risks? Does ERM staff work with business unit staff to assist with identifying risks?)*

2) Review the results of the most recent ERM staff recovery plan testing. *(Were the assumptions reasonable, and approved by management? Were the results reported to the board or board committee?)*

5. Conclusions

1) Summarize conclusions for all examination work performed, including work performed by other FHFA staff as it relates to the regulated entity's ERM function. Develop a memorandum describing the risks to the regulated entity resulting from the risks related to inadequate or inappropriate risk management. The memorandum should describe the basis of conclusions reached and summarize the analysis completed. Within the memorandum, discuss the types of 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.

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) Draft a conclusions letter (for Enterprise examinations) and prepare findings memoranda (for FHLBank or OF examinations), as appropriate. Findings should identify the most significant risks to the regulated entity and the potential impacts to the regulated entity resulting from the concerns identified. Significant findings should describe a specific end result that will resolve the issue. Communicate preliminary conclusions and findings, if applicable, to the EIC. Discuss conclusions and findings, if applicable, with regulated entity personnel to confirm the analysis and findings are free of factual errors.

4) Develop a list of follow-up items to evaluate during the next examination. In addition to findings developed in the steps above (if any), 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 regulated entity's practices or anticipated external changes that could affect the regulated entity's future oversight of ERM practices.