

---

## Introduction

Enterprise-wide Risk Management (ERM) is a risk management concept that has evolved into an essential element of an organization's overall risk management practices. It is critical to an assessment of current and potential risks and the establishment of an organization's risk tolerance. ERM's primary objective is to identify, measure, monitor, and report on risk exposures on an ongoing basis. Its purview should encompass all on- and off-balance sheet risks at entity-wide, portfolio, and business-line levels. The ERM function should take into account the extent to which risks overlap or are interrelated. ERM evaluates decisions made to accept a particular risk and assesses the aggregate level of risk in the institution in relation to the risk tolerance established by the board of directors. This examination module is applicable in the examination of the Enterprises (Fannie Mae and Freddie Mac), the Federal Home Loan Banks (FHLBanks) (the FHLBanks, Fannie Mae, and Freddie Mac are referred to collectively as the regulated entities), and the Office of Finance.

Effective ERM helps management achieve the regulated entity's performance and profitability targets and prevent loss of resources. ERM can also ensure appropriate reporting and compliance with laws and regulations, and avoid damage to the institution's reputation and associated consequences. Sound practices for effective ERM can provide the following benefits:<sup>1</sup>

- 1) *Align risk appetite and strategy.* Management should consider the institution's risk appetite, as established by the board of directors, in evaluating strategic alternatives, setting related objectives, establishing and defining risk tolerances, and developing mechanisms to manage related risks.
- 2) *Enhance risk response decisions.* Effective ERM can provide the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- 3) *Reduce operational surprises and losses.* Institutions can gain enhanced capabilities to identify potential events and establish responses, reducing surprises and associated costs or losses.
- 4) *Identify and manage multiple and cross-enterprise risks.* Every institution faces a myriad of risks affecting different parts of the organization. Effective ERM facilitates effective response to the interrelated effects and integrated responses to multiple risks.

---

<sup>1</sup> Source: Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management—Integrated Framework* (September 2004).

- 
- 5) *Seizing opportunities.* By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
  - 6) *Improving deployment of capital.* Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

### *ERM Structure and Function*

The ERM structure should promote organizational awareness and help shape the culture regarding risk acceptance and control. While no uniform ERM structure is appropriate for all institutions, ERM should incorporate the following key features:

- 1) Independence is crucial. ERM must have the authority to identify, measure, monitor, and report on all risks across the institution. It should enjoy free access to all information, and should exclude no business line or activity from its oversight. ERM must be able to communicate freely to the board of directors and senior management. The ERM function must not be involved in any risk taking activity, nor should its budget or compensation program be affected by risk levels or business unit metrics. While it is not uncommon for risk managers to work closely with business units or line managers, risk managers should be independent of the business unit whose activities he/she reviews.
- 2) ERM must have an effective reporting system to both provide and obtain information. ERM should have processes in place to report to the board of directors and senior management on a routine basis. ERM reports should be a part of the materials prepared for the board of director's regular meetings and should incorporate performance measures compared to defined risk tolerances. ERM should provide summary reports about specific reviews to the board of directors along with management's response.

ERM must establish a management information system to ensure it receives the data it needs to conduct its risk monitoring duty and to document its own performance so that it may be independently reviewed. ERM should receive accurate and timely performance data from each business unit or function sufficient for regular monitoring.

- 3) The institution should ensure through its planning and budgeting processes that ERM has adequate resources (in both number and quality), access to information technology systems and systems development resources, and support and access to internal information. Compensation and other incentives (e.g., opportunities for promotion) for all ERM staff should be sufficient to attract and retain qualified personnel.

- 
- 4) ERM personnel should possess sufficient experience and qualifications, including market and product knowledge, and risk disciplines. Staff should have the competence to question and, when appropriate, challenge business practices that result in inappropriate risk to the institution.
  - 5) ERM must have sufficient authority within the institution to bring issues raised by risk managers to the attention of the board of directors, senior management, and business line staff. Proper positioning and support of ERM helps ensure that the views of risk managers are a part of business decisions.
  - 6) ERM activities should be effective. In order to assess effectiveness, there should be evidence and documentation that the institution has changed its policies or practices in a manner that addresses concerns raised by the ERM function.

*Chief Risk Officer*

- 1) Institutions must have an independent senior executive with responsibility for the risk management function and the regulated entity's ERM framework. Financial institutions commonly refer to this position as the chief risk officer (CRO). Whatever the title, the role of the CRO should be distinct from other executive functions and business line responsibilities. Given the nature of the CRO's responsibilities, there generally should be no "dual hatting;" that is, the chief operating officer, chief financial officer (CFO), chief auditor, or other senior management should not also exercise the responsibilities of the CRO.
- 2) The CRO is responsible for the ERM framework, the underlying policies, major procedures, risk reporting, and overall management of the framework. Managing and controlling risk is the responsibility of line or business unit personnel. While the CRO is independent of risk-taking, he or she must be knowledgeable of business functions. The CRO should work with business unit managers to establish effective risk management practices. Each business function within an institution is accountable for risk management. Business units need to have resident expertise on the processes performed while ERM provides the operating framework.

Other CRO responsibilities may include:

- a) Establishing ERM policies.
- b) Overseeing the development of entity-wide and specific business unit risk tolerance thresholds.
- c) Recommending or evaluating corrective actions.
- d) Managing the activities of the ERM function.
- e) Evaluating ERM personnel.

- 
- 3) The CRO is part of the management team, unlike the role of the internal audit director, which is independent of executive management. The role of the CRO should not be shared by the internal audit director or otherwise comingled with the internal audit function.
  - 4) The CRO should have sufficient independence, stature, and authority within the organization. Beyond periodic reporting, the CRO should have access to the board of directors and senior management on key risk issues and be empowered to obtain information he or she deems necessary. Such interactions should not compromise the CRO's independence.
  - 5) The CRO should report directly to the chief executive officer (CEO) and the risk committee of the board of directors. The CRO must provide periodic reporting to the board of directors on compliance with, and the adequacy of, current risk management policies and procedures of the institution, and recommend any adjustments to such policies and procedures that are necessary and appropriate. CRO reports should also contain information on the level and trend of the institution's risk exposures. The CRO should meet with the board in executive session on a routine basis to ensure the CRO is able to discuss matters free from management's influence.

The sophistication of the institution's ERM program should keep pace with developments at the institution such as balance sheet and revenue growth, increasing complexity of the institution's business, and operating structure. ERM planning, and periodic review of such plans, should take these factors into account. Moreover, the ERM function should be responsive to changes in the overall economy and the housing market.

The board of directors should have regular interaction with the CRO. The board may delegate these responsibilities to a committee of the board. When evaluating the appropriateness of such delegation, the examiner should consider whether the board members on the committee have the skills necessary to ensure an effective and independent ERM function is in place.

### **Regulatory Environment**

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

- 1) ***Rules and Regulations of the Federal Housing Finance Agency (FHFA) and its predecessors, the Federal Housing Finance Board (Finance Board) and the Office of Federal Housing Enterprise Oversight (OFHEO), include the following parts and sections relevant to Enterprise-wide Risk Management:***

12 CFR Part 1236 of FHFA's regulations, and the Appendix to Part 1236—Prudential

---

Management and Operations Standards, establish the agency's prudential management and operations standards (PMOS), and contain guidelines for risk management processes. Specifically, 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.

12 CFR 917.3 of the Finance Board's regulations addresses risk management and requires the board of directors to, among other things, adopt a risk management policy, review the risk management policy at least annually, and re-adopt the policy not less often than every three years. (12 CFR 917.3(a)) In addition, senior management of each FHLBank must perform a written risk assessment at least annually that is reasonably designed to identify and evaluate all material risks that could adversely affect the achievement of the FHLBank's performance objectives and compliance requirements. The board of directors must review the risk assessment promptly after the assessment is completed. (12 CFR 917.3(c))

12 CFR 1710.19(b) of the OFHEO regulations addresses risk management programs and states:

“Risk management program. (1) An Enterprise shall establish and maintain a risk management program that is reasonably designed to manage the risks of the operations of the Enterprise. (2) The risk management program shall be headed by a risk management officer, however styled, who reports directly to the chief executive officer of the Enterprise. The risk management officer shall report regularly to the board of directors or an appropriate committee of the board of directors on compliance with and the adequacy of current risk management policies and procedures of the Enterprise, and shall recommend any adjustments to such policies and procedures that he or she considers necessary and appropriate.”

**2) *Examination Guidance of the Office of Federal Housing Enterprise Oversight that provides guidance relating to Enterprise-wide Risk Management include the following:***

PG-06-001, Examination for Corporate Governance, dated November 8, 2006, sets forth guidance and standards relating to the corporate governance of the Enterprises consistent with the safety and soundness responsibilities of OFHEO under the Federal Housing Enterprises Financial Safety and Soundness Act of 1992 and the OFHEO corporate governance regulation, 12 CFR Part 1710. The policy guidance sets forth requirements regarding the establishment of a risk management program, the employment or removal of the CRO, and the

---

independence of the CRO and the reporting structure under which the CRO operates. The guidance also details the functions and responsibilities of the CRO.

**3) *Advisory Bulletins of the Federal Housing Finance Board that provide guidance relating to Enterprise-wide Risk Management include the following:***

Advisory Bulletin 2005-05, dated May 18, 2005, discusses the responsibilities of the ERM function, including reporting requirements, independence, and authority. Refer to the Issues Specific to the FHLBanks and the Office of Finance section below for further information.

**4) *Other sources of sound professional practices for Enterprise-wide Risk Management and corporate governance that examiners may consider when evaluating Enterprise-wide Risk Management practices include the following:***

Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a joint initiative among the Institute of Internal Auditors, American Institute of Certified Public Accountants, American Accounting Association, Financial Executives International, and the National Association of Accountants (now the Institute of Management Accountants) that develops frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. COSO materials are instructive sources of sound practice; however, they are not authoritative and must be considered relative to FHFA regulations and supervisory guidelines.

Bank for International Settlements, Basel Committee on Banking Supervision (Basel Committee). The Basel Committee provides a forum for international cooperation on banking supervisory matters, and publishes materials that promote sound risk management practices. Basel Committee materials are instructive sources of sound practice, however, they are not authoritative, and must be considered relative to FHFA regulations and supervisory guidelines.

**Issues Specific to the Regulated Entities and the Office of Finance**

The Enterprises and the FHLBanks currently operate under two different corporate governance regulations, although FHFA is in process of establishing one unified regulation to apply to all regulated entities. Examiners should note that differences will exist in corporate governance requirements until such time as this regulation is finalized. Below summarizes the important aspects of each regulation and related guidance, although examiners should familiarize themselves all aspects of each regulation and related guidance.

---

**Issues Specific to the Enterprises**

In accordance with 12 CFR 1710.19, an Enterprise is required to establish and maintain a risk management program that is reasonably designed to manage the risks of the operations of the Enterprise. The risk management program shall be headed by a risk management officer, however styled, who reports directly to the CEO of the Enterprise. The risk management officer shall report regularly to the board of directors or an appropriate committee of the board of directors on compliance with and the adequacy of current risk management policies and procedures of the Enterprise, and shall recommend any adjustments to such policies and procedures that he or she considers necessary and appropriate.

PG-06-001, entitled Examination for Corporate Governance, sets forth examination guidance and standards relating to corporate governance and, and specifically, the risk management program. PG-06-001 states that the head of the risk management office (CRO) may be employed or removed from employment only upon approval of the board of directors. The CRO should be independent of the CFO and report directly to the CEO and independently to the board committee responsible for risk. The head of each group responsible for oversight of market risk, credit risk, or operational risk should report directly to the CRO.

OFHEO Examination Guidance PG-06-001 also discusses the functions and responsibilities of the CRO. Specifically, the CRO should, at a minimum:

- 1) Provide overall leadership, vision, and direction for ERM including implementing a framework to manage all aspects of risk, ensuring that risk management activities are appropriate to the level of risk assumed, and developing risk management policies.
- 2) Maintain risk management readiness by establishing or reviewing communication and training programs, risk-based performance measurement and incentives, and other programs.
- 3) Assure that risk is properly identified, measured, prioritized, managed, and reported at business and corporate levels; and that risk is properly understood and translated into meaningful business requirements, objectives, and metrics.
- 4) Assure the establishment of systems which are reasonably designed to assure that business units are fully engaged in managing their portion of the risk and are accountable.
- 5) In support of the risk management program, assure the development of risk technologies and of analytical, systems, and data management capabilities; and the implementation of risk metrics and reports, including losses and incidents, key risk exposures, and early warning indicators.

---

**Issues Specific to the FHLBanks and the Office of Finance**

In accordance with 12 CFR 917.3, an FHLBank is required to have in effect at all times a risk management policy that addresses the FHLBank's exposure to credit risk, market risk, liquidity risk, business risk and operations risk. In addition, senior management of each FHLBank shall perform, at least annually, a risk assessment that is reasonably designed to identify and evaluate all material risks, including both quantitative and qualitative aspects, that could adversely affect the achievement of the FHLBank's performance objectives and compliance requirements.

Advisory Bulletin 2005-05 sets forth guidance regarding the responsibilities of the ERM function. Specifically, it states that the process of identifying, measuring, monitoring, and reporting risk should be managed separately from business units and individuals conducting risk-taking activities. As a matter of sound practice, an FHLBank should have a risk management function or unit(s) with clearly defined responsibilities that reports directly to executive management and has regular reporting responsibility to the board of directors or a committee thereof. The risk management function should not report to business units that undertake risk positioning. The risk management function should have the authority to ensure:

- 1) The establishment of a framework for identifying, measuring, monitoring and reporting on financial (market and credit risks) and operational risks, *e.g.*, legal and reputation risks.
- 2) The development and maintenance of sound models for risk measurement.
- 3) The review and approval of pricing models and valuation systems used by front and back-office personnel.
- 4) The performance of model validation and effectiveness procedures.
- 5) The development of risk limit policies and the monitoring of positions for adherence to these policies.
- 6) The design of stress scenarios to measure the effects of unusual market conditions.
- 7) The monitoring of the variance between the actual volatility of portfolio value (profit and loss) and that predicted.
- 8) The reporting of risk exposures to senior management and the board of directors or a committee thereof on a regular basis.
- 9) The coordination of risk management with all business units of the Bank as a means of ensuring that all risks, including legal and reputation risks, are factored into the decision-making process.
- 10) The preparation of risk assessments.
- 11) The risk management function should be examined by the internal audit function to ensure that risk management objectives are being achieved.

---

**Examination Guidance**

The workprogram for the Enterprise-wide Risk Management 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 conclusions on the quantity of risk and quality of risk management pertaining to this area. Transaction testing is mandatory and the examiner must evidence 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 institution's ERM 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 ERM.
- 2) Review FHFA off-site monitoring or analysis reports, and workpapers produced as part of on-going monitoring, related to ERM.
- 3) Assess the status of outstanding Matters Requiring Attention and Violations pertaining to ERM.
- 4) Review internal audit reports for outstanding issues relating to ERM.
- 5) Review minutes of meetings of the board of directors and relevant board and management committees for any issues regarding ERM.
- 6) Identify the CRO, or equivalent, who heads the ERM function.
- 7) Review and evaluate the independence of the ERM function. (*Does the ERM function inappropriately include risk-taking activities?*)

- 8) Evaluate the ERM reporting structure to ensure it is appropriately aligned with business segments or risk positions.
- 9) Assess the stature of the CRO in the regulated entity's organizational structure. *(Does the CRO position report to the CEO, have independence and sufficient standing in the organization?)*
- 10) Determine if the purpose, authority, and responsibility of ERM have been formally defined in a charter that has been approved by the board of directors, or a board committee.
- 11) Determine if the charter establishes ERM's position within the institution; authorizes unrestricted access to records, personnel, and physical properties relevant to the performance of its duties; defines the scope of ERM activities; and is periodically reviewed by the board of directors or board committee.
- 12) Evaluate the adequacy of the scope and testing completed by ERM and determine the status of corrective actions for findings. *(Does ERM evaluate risks across the business units?)*
- 13) Assess the communications between the ERM and the board of directors, or board 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) Significant risk limits and/or risk tolerance levels, including ERM's judgment of the reasonableness of the limits and the consistency of the application of those limits across all business units.
  - c) Potential effects on the financial statements of any significant risks and exposures.
  - d) Risk limit or risk tolerance exceptions (approved or unapproved) and ERM's judgment concerning those exceptions.
  - e) Management approved overrides to risk limits or tolerances and ERM's judgment concerning those overrides.
  - f) Fraud and other illegal acts.
  - g) ERM's budget, strategy, and ability to complete its annual plan.
  - h) Material uncertainties related to events and conditions, including going concern issues.
  - i) Disagreements with management and difficulties encountered in performing ERM activities.
  - j) Major issues discussed with management.

---

Summarize the work performed in the examination of the ERM area. 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.

<b>2. Description of Risks</b>
--------------------------------

- 1) Determine whether the ERM function has taken appropriate action to identify, assess, and prioritize existing, emerging, and potential risks that could affect the achievement of the institution's strategies, goals, and objectives. Consider whether:
  - a) Business units identify risk based on both trends and the current operating environment.
  - b) Management solicits input and timely information from all parts of the organization when identifying risk and understanding how risks are related to one another.
  - c) Risk assessments are a formal and ongoing process throughout the organization, and if management across the institution uses common terminology to categorize risks into discrete categories.
  - d) There is consistency in the time horizon used to assess risk with the time horizon used to plan business strategy and objectives.
  - e) Management assesses overall risks to build a corporate risk profile.
  - f) The process for assessing key risks at all levels of the organization and across all businesses is consistent, standardized, and flexible (in order to respond to changing conditions that affect the institution's risk profile).
  
- 2) Assess the effectiveness of ERM strategy and action planning – the identification, design, and development of actions that will best address the risk and align with an institution's risk tolerance and risk appetite (e.g., risk optimization, risk retention, risk transfer). 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) Risk owners use a formal action-planning process that is monitored to completion.
  - d) Key risk owners identify alternative risk strategies and choose appropriate strategies based on a cost-benefit analysis.
  
- 3) Review and evaluate the institution's method for aggregating risks to develop a portfolio view of risk across the organization. Consider whether:

- 
- a) The process considers risks from both a business segment and entity-wide perspective.
  - b) ERM evaluates whether the institution's aggregated risk profile is commensurate with its overall risk appetite.
  - c) ERM performs adequate analyses to be used by the board of directors in assessing the institution's risks. (*Does ERM employ both qualitative and quantitative techniques appropriately? Does ERM utilize benchmarking or modeling techniques? If so, are assumptions reasonable and conclusions supported?*)
  - d) ERM considers the interplay and correlations among risks when evaluating and monitoring risks and action plans.
- 4) Evaluate risk measurement tools and techniques designed to support the ERM process across the institution. Consider whether:
- a) Risk measurement techniques employed by the institution (scenario planning, Earnings-at-Risk, Value-at-Risk, etc.) are commensurate with risk complexity and that risk exposures are calculated using qualitative as well as quantitative data.
  - b) The risk assessment process stress tests the key assumptions of risk models.
- 5) Evaluate how ERM uses risk self-assessments to implement the risk management framework.
- 6) Evaluate the self-assessment process. Consider the following:
- a) Timing and frequency.
  - b) Quality control of assessments.
  - c) Consistency of measures and analytical approaches.
  - d) Evidence of effectiveness (changes in activities).
- 7) Verify that new products are captured in the risk assessment process.

<b>3. Risk Management</b>
---------------------------

*Organizational Structure*

- 1) Review the organizational structure and determine if the CRO reports directly to the CEO and provides periodic reports to the board of directors, and/or a committee of the board. Determine whether the CRO has direct access to the board of directors. (*Is the CRO sufficiently independent of influences from the risk-taking functions?*)
- 2) Identify any personnel within ERM who also have reporting lines to or from business unit personnel; evaluate the appropriateness of this reporting structure as it affects the

---

independence of ERM.

- 3) Determine and assess how the independence of risk managers who work closely with business line personnel is maintained. Consider the following:
  - a) Performance evaluation process.
  - b) Compensation and/or bonus goals.
  - c) Evidence of changed activity.
- 4) Determine how decisions related to ERM are made and responsibilities assigned.
  - a) Determine if the board of directors requires and receives formal updates on aggregate and key business segment risks on a periodic basis.
  - b) Assess the timeliness of the information the board of directors receives on changing risk profiles, including new or additional risks.
  - c) Determine whether risk ownership of business units reside at a senior management level within the organization.
  - d) Determine whether the internal audit function regularly evaluates the ERM function and established risk management processes against management's established standards for each component.
  - e) Determine if structured activities related to risk management are included in formalized charters (e.g., board of directors or respective board committee).
  - f) Assess ERM's human and capital resources.
- 5) Assess the overall competency and skill sets of the CRO and ERM staff. At a minimum, consider experience, tenure in position, education, and professional certifications. *(Does the ERM staff have sufficient product knowledge? Is there a program of continuing education for the ERM staff?)*
- 6) Evaluate the existence and effectiveness of ERM training and awareness. *(Are the skills of the ERM staff commensurate with current and emerging risks?)*
- 7) Determine the extent to which risk identification, monitoring, and remediation are factored into management's performance evaluations.
- 8) Determine how ERM maintains contact with business units or operational functions. Consider the following:
  - a) If risk management personnel are directly placed with business units, or with operational areas reporting to the risk management office.
  - b) If the CRO is a voting member on management-level risk committees. *(Does the CRO act independently within the framework of such committees to ensure adherence to appropriate risk limits?)*

- 
- c) The existence of business-line or operational unit personnel with indirect reporting lines to the risk management department.
  - d) The existence of an independent review function within the risk management department that conducts periodic, or continuous, assessments of business-line or operational 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 ongoing monitoring responsibilities are clearly established.
  - d) Whether policies related to specific risk areas (e.g., market risk, operational risk) are communicated and enforced across the regulated entity.
  - e) Whether risk metrics are appropriate.
  - f) Whether ERM policies are periodically reviewed to ensure alignment with board of directors' policies and limits.
  - g) Whether the board of directors, internal audit, compliance, and legal personnel review ERM policies on a regular basis to ensure compliance with laws and regulations and to ensure that policies are revised as processes are changed to mitigate risks.
- 2) Determine if there are established communication channels between 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 organization?*)
- 3) Determine whether the ERM program provides for continuous improvement and a process of evaluating results and re-aligning efforts and resources to optimize the regulated entity's risk management activities.
- 4) Assess the adequacy of the institution's risk analysis and risk measurement approaches. Consider whether:
  - a) Qualitative approaches are used, where appropriate, to measure the effect of risk (i.e., subject matter experts, scenario analysis, record keeping, interviews, or surveys).
  - b) Root cause analyses are performed for key risks.
  - c) Risk owners evaluate and provide ERM with feedback on the effectiveness of the existing risk management activities and exposure level measurements.
  - d) Risk assessment measurements are aligned with the institution's risk tolerance metrics and business performance measures.

- 5) Review and evaluate the institution's formal integration of risk management activities into key decision-making processes. Consider whether:
  - a) Management decisions are based upon tolerances, appetites, and potential effects of risks on strategies, goals, and objectives.
  - b) ERM tools and methods are used to support strategic planning, annual budgeting, and the daily strategic and operational decisions, enabling business performance to be evaluated on a consistent risk-adjusted basis.
- 6) Evaluate how the risk management function uses the risk 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 board of directors' risk appetite and individual risk limits. Consider the following:
  - a) Processes for establishing risk tolerances and risk limits.
  - b) The comprehensiveness of the CRO's assessment of risks to the board of directors.
  - c) The effect of the information provided by the CRO in establishing risk limits.
  - d) Comprehensiveness of risk limits.
  - e) Documentation in meeting minutes of the board of directors or board committee deliberations on risk limits.
  - f) Scope and thoroughness of risk evaluations.
  - g) Clarity, timeliness, and completeness of risk reporting to the board of directors.
- 2) Evaluate management's efforts to set appropriate risk limits, establish controls, and implement risk offset activities. (*Are risk limits and controls in-line with the risk appetite established by the board?*)

*Reporting*

- 1) Assess management's risk reporting practices. Consider both internal documentation practices and reporting to senior management.
- 2) Review and evaluate the quality and frequency of ERM reports presented to the board of directors. Consider whether:

- 
- a) The board of directors monitors key risks using specific metrics and standardized reports that evaluate the effectiveness of the institution's risk management strategies, actions, and processes.
  - b) Performance indicators/risk indicators are established, monitored, and reported on a continuous basis for key risks.
  - c) Risk interdependencies are measured and reported.
  - d) The reports focus on past trends or address emerging risks.
  - e) The reports link to the achievement of business unit and entity-wide strategies, goals, and objectives.
- 3) Review the minutes of the board of directors or the relevant board committee meetings to determine if the information reported by ERM 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) Evaluate the extent to which the internal auditors' assess the ERM function. (*Do internal auditors periodically evaluate the effectiveness of the ERM function? Does the review include the ERM processes, the effectiveness and efficiency of risk responses and related control activities, and the completeness and accuracy of ERM reporting?*)

*Information Technology*

- 1) Determine if the ERM function conducts periodic assessments of its management information system (MIS) and reporting packages. If so, obtain the assessments and assess any identified weaknesses and required follow up actions taken by management.
- 2) Evaluate the flexibility of ERM MIS systems and reporting. Determine if ERM management can obtain *ad hoc* reports when needed to evaluate risk.

*Compliance*

- 1) Assess compliance with Standard 8 of FHFA's PMOS guidelines (PMOS apply only to the regulated entities; they do not apply to the Office of Finance). Specifically:
  - a) Determine if the board of directors has ensured that senior management includes properly trained and competent individuals to oversee the institution's risk management process. (Principle 1)
  - b) Determine if the requisite processes are in place to identify, manage, monitor, and control the institution's risk exposures on a business unit and an enterprise-wide basis. (Principle 1)

- 
- c) Determine if the board of directors has approved the institution's major risk limits. (Principle 1)
  - d) Determine if the board of directors has ensured that incentive compensation measures for senior management capture a full range of risk exposures and is not solely tied to operating efficiency measures, such as profits or dividends. (Principle 1)
  - e) Evaluate the board of director's and senior management's role in establishing an organizational awareness and culture that promotes effective ERM. (Principle 2)
  - f) Determine if the board of directors and senior management are provided with accurate, timely, and informative risk reports on a regular basis that provide an overview of the institution's overall risk profile, including its exposures to market, credit, liquidity, and operational risk and any concentration of risk. (Principle 2)
  - g) Determine if the board of directors and senior management have ensured that the institution's overall risk profile is aligned with its mission objectives. (Principle 2)
  - h) Determine if the board of directors and senior management have ensured that the institution performs a comprehensive risk self-assessment on an annual basis to identify and evaluate all material risks. (Principle 2)
  - i) Determine if the institution has an independent risk management function, or unit, with responsibility for risk measurement and risk monitoring, including monitoring and enforcement of risk limits. (Principle 3)
  - j) Determine if the CRO heads the risk management function. (Principle 4)
  - k) Determine if the CRO reports directly to the CEO and provides reports to the board of directors or a committee of the board. (Principle 5)
  - l) Determine if the risk management function has adequate resources, including a well-trained and capable staff. (Principle 6)
  - m) Determine if the institution measures, monitors, and controls its overall risk exposures, reviewing market, credit, liquidity, and operational risk exposures on both a business unit (or business segment) and enterprise-wide basis. (Principle 7)
  - n) Determine if the institution has the risk management systems to generate, at an appropriate frequency, the information needed to manage risk. Such systems should include systems for market, credit, and liquidity risk analysis, asset and liability management, regulatory reporting, and performance measurement. (Principle 8)
  - o) Determine if the institution has a comprehensive set of risk limits and monitoring procedures to ensure that risk exposures remain within established risk limits, and a mechanism for reporting violations and breaches of risk limits to senior management and the board of directors. (Principle 9)
  - p) Determine if the institution has sufficient controls around risk measurement models to ensure the completeness, accuracy, and timeliness of risk information. (Principle 10)

- 
- q) Determine if the institution has adequate and well-tested disaster recovery and business resumption plans for all major systems and has remote facilities to limit the effect of disruptive events. (Principle 11)
  - r) Determine if the institution is in compliance with applicable laws, regulations, and policies (i.e., guidance documents and advisory bulletins) governing the management of risk. (Principle 12)

#### **4. Testing**

- 1) Select a sample of recently completed risk self-assessments and evaluate the adequacy, consistency, and timing of the assessments. *(Do the risk assessments identify all major risks?)*
- 2) Determine if any action was taken as a result of any assessments and the status of corrective actions.
- 3) Evaluate the adequacy of the objectives and scopes of reviews performed by any outside consultants and determine the status of management's actions regarding recommendations. *(Did management take appropriate action in response to consultant recommendations?)*
- 4) Assess the adequacy of ERM's work in evaluating the effectiveness of the institution's risk control environment, particularly the identification and management of the principal risks facing the regulated entity.
- 5) Review ERM resumes to determine if education, experience, training, and professional certifications indicate that ERM personnel are qualified to perform their duties and responsibilities.
- 6) Interview ERM staff to determine if they have sufficient knowledge and understanding of key risks and controls.
- 7) Review and evaluate on-going ERM training programs to address the continuing professional development of ERM personnel.

#### **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 institution which the ERM function attempts to address and conclude on the appropriateness of the regulated entity's management of those risks. The memorandum should describe the basis of conclusions reached and summarize the analysis completed. Within the memorandum, discuss the types of risk the institution's ERM function may expose the institution to (e.g., market, credit, operational); 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 institution's response to previous examination findings and concerns.
- 3) Develop examination findings and prepare findings memorandums, 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 institution 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 institution to remediate the finding. Communicate preliminary findings to the EIC. Discuss findings with personnel at the institution to ensure the findings and analysis 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 institution 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 oversight of the ERM function.

---

**Workprogram**

**1. Scope of Examination Work Performed**

Workpapers must document the examination activities undertaken to evaluate potential risks related to Enterprise-wide Risk Management.

**2. Description of Risks**

- Identify areas of concern related to Enterprise-wide Risk Management
- Assess current risks and trends in the risk to the institution associated with of Enterprise-wide Risk Management
- Evaluate changes within the institution or industry affecting risk
- Evaluate the institution's risk-identification practices and conclude on their adequacy

**3. Risk Management**

- Assess and conclude on the adequacy of the institution's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
  - The institution's organizational structure
  - Policy and procedure development for this area
  - Appropriateness of risk metrics established in this area
  - Reporting by management and the board
- Assess and conclude on the internal and external audit of risks
- Assess and conclude on the adequacy of information technology and controls related to Enterprise-wide Risk Management
- Assess and conclude on the adequacy of the institution'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 Enterprise-wide Risk Management
  - Conclude on the level of risk to the institution
  - Include an assessment of the adequacy of an institution's monitoring of risk and establishment of internal controls to mitigate risk
- Conclude on responsiveness to examination findings from previous examinations
- Develop findings, as appropriate
- Identify areas requiring follow-up examination activities or monitoring