Table of Contents

Introduction

Insurance is an important risk management tool and is frequently used to protect the Federal Home Loan Banks (FHLBanks), Fannie Mae, and Freddie Mac (collectively, the regulated entities) and the Office of Finance (OF) from operational losses. Although the regulated entities use some forms of insurance to mitigate credit risk, insurance as discussed in this module is primarily used to mitigate operational risk. The potential for liability arising from the FHLBank's operations and system of controls must be reflected in the annual risk assessment required to be conducted pursuant to 12 CFR 917.3 of the former Federal Housing Finance Board (Finance Board) regulations. Fannie Mae and Freddie Mac may also conduct regular risk assessments. Risk assessments should clearly support why and how the regulated entity is, or is not, taking advantage of insurance as a risk mitigation tool.

The value of insurance lies in the protection it affords from losses arising from risk control failures or from other causes. The specific insurance needs must be assessed on a case-by-case basis; only by reviewing each policy in force can the actual degree of coverage and protection be determined. In addition, insurance management should be reflected in the regulated entity's and OF's business continuity plans as the potential for losses and errors may increase due to a disabling event.

The objective of an insurance management program is to minimize losses and costs arising from certain operating risks undertaken by the regulated entity or OF, such as direct costs of loss prevention measures, insurance premiums, losses sustained, and related administrative expenses. The board of directors and senior management must determine the maximum loss the regulated entity or OF is willing to accept and must, at a minimum, perform and document an annual review of the insurance management program. The maintenance of adequate insurance should not, by itself, be viewed as a satisfactory substitute for the other elements of a sound risk management program. Furthermore, each regulated entity and the OF should establish standards for when insurance coverage is needed and establish criteria for appropriate insurance coverage.

Types of Insurance

The insurance industry offers various types of coverages that can be purchased. Those coverages include, but are not limited to, the following:

1) *Fidelity Bond Coverage* is designed to protect a regulated entity or the OF from catastrophic losses resulting from dishonest or fraudulent acts of directors, officers, employees, agents, and unrelated third-parties, which include losses arising from:

    a) Defalcations;
    b) Use of forged documents;
    c) Circulation of false securities;
    d) Circulation of counterfeit money; and
    e) Other criminal acts.

Customarily, a fidelity bond will contain a termination clause that should be reviewed by personnel responsible for the administration of the insurance management program and by legal counsel. Management must have a good understanding of the circumstances under which the underwriter may terminate the bond's coverage.

2) *Directors and Officers (D&O) Liability Insurance* provides coverage for the indemnification of directors, officers, and other employees against legal and other expenses incurred in defending lawsuits related to the performance of their official duties. Such insurance does not cover instances of crime or dishonesty, personal gain, or apparent conflicts of interest.

   Levels of D&O coverage include the following:

   a) *Side A* reimburses officers and directors to the extent that they are not indemnified by the company;
   b) *Side B* reimburses a company for amounts spent to indemnify directors and officers for costs, settlements and judgments, subject to a deductible or "retention"; and
   c) *Side C* indemnifies a company against its own liability in connection with securities claims, subject to deductible or retention.

3) *Banker's Professional Liability Insurance (Errors and Omissions Insurance)* provides coverage to a company against loss from a customer's claim of negligent acts, errors or omissions in the performance of professional services. This may include loss of client data, software or system failure, and failure to perform professional duties.

   An errors and omissions liability policy protects the regulated entity and the OF, directors, officers, and employees from loss in instances where there is a written agreement between the regulated entity or the OF and a customer to provide professional services to the customer for a fee, or other monetary consideration, or where a fee or other monetary consideration would usually be received, but for business or other reasons, the fee has been waived.

   In addition to maintaining an errors and omissions liability policy to protect the regulated entity or OF from its own acts of negligence, errors and omissions in the provision of services to its own customers, each regulated entity and the OF should require that third-party vendors with whom it contracts for services maintain adequate coverage under their own error and omissions liability policy and fidelity bonds to protect the regulated entity against loss in the event of negligent acts, errors, and omissions on the part of the third-party vendor in providing services to the regulated entity or the OF. Each regulated entity and the OF should perform a thorough review of the vendor's policy coverages, exclusions, and limitations prior to entering into any agreement with any vendor providing a service to the regulated entity or the OF. For example, coverage may not be provided for information technology consultants and contractors who perform services on behalf of the regulated entity or the OF.

Therefore, during the consultant/vendor selection process, each regulated entity and the OF should require the consultant/vendor to provide a full analysis of the coverages, exclusions, and limitations contained in the errors and omissions insurance policy and fidelity bond. See the Examination Manual module *Third Party Relationship Management* for additional information about vendor management.

4) *Commercial General Liability Insurance* provides coverage for bodily injury occurring on a regulated entity's or the OF's premises.

5) *Property Insurance* provides coverage for the theft or destruction of a regulated entity's or the OF's property and fixed assets such as computer hardware, software, and other office furnishings and equipment, up to a specified amount. Policy coverage should include "hot sites" critical to the maintenance of business continuity.

   Regulated entity or OF personnel responsible for the administration of the insurance management program should be aware of and follow the requirements for notifying the insurance agent/broker to adjust policy coverage to ensure the adequacy of coverage for newly purchased or leased items. A purchased or leased item will only be insured within the general limits of a property insurance policy unless it has been placed on a specific schedule within the policy that provides for extra insurance coverage above the general policy limits for that item. For example:

   a) Furniture and owned equipment are usually not specifically scheduled with an insurer, so any claim for items lost, stolen, or damaged would be based on the general policy limits.

   b) Leased equipment is usually required by the lessor to be specifically scheduled with an insurer. If new equipment is leased, the insurer is notified of the new schedule and dollar amount, endorses the additional schedule on the certificate of insurance to the lessor, and sends the lessor a new certificate of insurance as required by the equipment lease.

6) *Valuable Papers and Records Insurance* provides coverage for the replacement of valuable papers and records, including those generated by electronic media.

7) *Automobile Public Liability and Property Damage Insurance* indemnifies a regulated entity or the OF against property and liability losses arising from injury or death when an owned, leased, or rented vehicle is involved. Non-ownership liability insurance should be considered if officers or employees use their own vehicles for business purposes.

8) *Travel Accident Insurance* provides coverage to directors, officers, and employees on losses sustained because of accidental injury or death while traveling on business.

9) *Umbrella Liability Insurance* provides excess coverage over and above existing liability policies as well as basic coverage for most known risks not covered by existing liability insurance.

10) *Internet Liability Insurance* provides coverage against claims that the content and/or performance of a regulated entity's or the OF's website have adversely affected a customer's business.

11) *Computer Cyber Crime Insurance* is specialized coverage that is tailored to the specific needs of the regulated entity or the OF, including the technology that is being used and the level of risk of cyber crime involved. Traditional insurance policies such as standard property and commercial general liability may not adequately address the risks of cyber-attack or network security failure.

    Coverage for threats arising both inside (first party) and outside (third party) the regulated entity or OF can be obtained which include:

    a) Loss/corruption of data, which covers the destruction of information due to viruses, worms, and other malware;

    b) Business interruptions, which result in loss of income as a result of an attack on the regulated entity's or the OF's network that limits its ability to conduct business; and

    c) Liability costs such as defense costs, settlement costs, and punitive damages that may be incurred by the regulated entity or the OF as a result of:

        i. Breach of privacy due to theft of data;
        ii. Transmission of computer viruses, worms, and other malware, that causes financial loss to third parties; and
        iii. Failure of security, which causes network systems to be unavailable to third parties.

12) *Employment Practices Liability Insurance* provides coverage against claims alleging an employment practices violation arising from wrongful dismissal, discharge, or termination; harassment; discrimination; employment-related misrepresentation; libel; slander; defamation; or wrongful discipline.

13) *Employee Benefit Plan Fiduciary Liability Insurance* provides coverage for specific wrongful acts as a fiduciary or as an administrator of the specified employee benefit plans.

14) *Terrorism Insurance* is specialized coverage for losses incurred due to terrorist acts.

15) *Kidnapping, Ransom and Extortion Insurance* is specialized coverage for employees who travel extensively overseas, have high profiles, handle large amounts of cash, or

work with sensitive information or technology. The coverage includes international support crisis management, dedicated phone lines, and professionals who will try to resolve or diffuse incidents or situations with the least harm to the employee.

16) *Key Person Insurance* insures the regulated entity and the OF on the life of an officer when the death of such officer, or key person, would be of such consequence as to give the regulated entity or the OF an insurable interest.

Primary Risks associated with an Insurance Management Program

The primary risks arising in connection with a regulated entity's or the OF's insurance management program include the following:

1) Lack of Sound Corporate Governance (Board of Directors and Senior Management Oversight)

a) Key risks and controls are not adequately identified, assessed, and monitored.
b) Information technology is not aligned with the regulated entity's or the OF's goals and strategies.
c) Responsibility for the operation of the insurance management program has not been assigned.
d) Assigned personnel do not have sufficient knowledge and technical expertise to manage the insurance management program.
e) An assessment of the adequacy of the insurance management program (including specific coverages, exclusions, limitations, current trends/developments) and costs is not communicated to senior management and the board of directors.
f) Background criminal and credit investigations are not performed on personnel prior to their retention. For key personnel, periodic credit investigations are not performed and mandatory leave policies (e.g., one week with a different individual performing the duties of the key person) have not been established and/or enforced.
g) Duties, responsibilities, and liabilities are not adequately addressed with vendors.
h) The regulated entity's or the OF's business continuity plan does not address the availability of insurance coverages in the event of a disruption in the regulated entity's or the OF's business.
i) Internal control weaknesses potentially affecting financial reporting have not been adequately identified, assessed, and disclosed.
j) Independent audit coverage and testing is limited; auditors are inexperienced or lack the technical expertise to test the control environment.
k) Low probability catastrophic risks that potentially could be insured at reasonable cost are not subject to documented reviews on a periodic basis.

2) Operational Risk

a) Inadequate coordination with the insurance agent/broker on trends, new issues/developments, claims histories, and current coverage affecting the

regulated entity or the OF.

b) Lack of a periodic assessment to determine the adequacy of insurance coverage, taking into account accompanying exclusions, limitations, and costs.
c) Inadequate coordination by insurance management functions with the other key operating areas with respect to insurance coverage and accompanying exclusions, limitations, and notification requirements.
d) Failure to adequately address duties, responsibilities, and liabilities with vendors.
e) Failure of the business continuity plan to address insurance considerations.
f) Lack of compliance with internal controls, policies, procedures, and specific requirements of the insurance policies, resulting in rejection of claims by insurers and incurrence of losses by the regulated entity or the OF.

Control Practices

A regulated entity's and the OF's control practices relating to the insurance management program should incorporate the practices set forth below:

1) Corporate Governance

Insurance management is utilized as a risk management tool to mitigate operational risk. Specific attributes include risk identification and analysis, risk control, and risk treatment (retaining or transferring the risk). The board and senior management must determine the maximum loss the regulated entity or the OF is able and willing to assume and perform an annual review of risk management and insurance programs.

2) Business Continuity

The business continuity plan should address the availability of insurance in the event of a disruption in the regulated entity's or the OF's business. The potential for losses and errors may increase due to a disabling event. For example, due to a disabling event, personnel may have to process wire transfer transactions in a manual environment, thereby increasing the possibility for losses due to errors and fraud.

The entity may mitigate risks and liability with the purchase of specific insurance and bond coverage such as directors' and officers' liability, errors and omissions, computer cyber crime, and fidelity bond coverage.

In addition, the specific limitations, exclusions, notifications, and other clauses of each policy should be reviewed to determine their effects upon the availability of coverage under specific circumstances. Claims may be rejected if weak controls or failure to follow established internal procedures are determined.

Regulatory Environment

The primary rules, regulations, standards, and guidance governing insurance management are set forth below. The examiner should ensure that the application of such authorities to a regulated entity or the OF has been considered by the regulated entity or the OF and its legal counsel.

1) Laws and Statutes pertaining to insurance management:

12 U.S.C 4520(b) - Federal Housing Enterprises Financial Safety and Soundness Act of 1992, as amended, requires the regulated entities to develop and implement standards and procedures to ensure, to the maximum extent possible, the inclusion and utilization of minorities in all business and activities of the regulated entity at all levels, including insurance and all types of contracts. The processes established by each regulated entity for review and evaluation for contract proposals and to hire service providers shall include a component that gives consideration to the diversity of the applicant.

2) Rules and Regulations of the Federal Housing Finance Agency (FHFA), which include parts and sections relevant to insurance management:

12 CFR Part 1236 Prudential Management and Operations Standards (PMOS) – PMOS Standards 1 and 8 highlight the need for the regulated entities to establish appropriate internal controls, including an adequate information technology system and sound risk management processes.

3) Rules and Regulations of the predecessor Office of Federal Housing Enterprise Oversight (OFHEO), which include the following parts and sections relevant to the Enterprises' insurance management:

12 CFR 1710.19 of OFHEO's regulations – Compliance and risk management programs; compliance with other laws provides that each Enterprise shall establish and maintain a risk management program that is reasonably designed to manage the risks of the operations of the Enterprise.

12 CFR 1720 – Safety and Soundness, Appendix A provides policy guidance with respect to minimum safety and soundness requirements.

4) Rules and Regulations of the predecessor Federal Housing Finance Board (Finance Board), which include the following parts and sections relevant to the FHLBanks' and the Office of Finance's insurance management:

12 CFR 917 of the Finance Board's regulations – Powers and Responsibilities of Bank Boards of Directors and Senior Management. In particular, 12 CFR 917.3, Risk Management, and 917.6, Internal Control System, are pertinent.

5) Advisory Bulletin of the Federal Housing Finance Agency that provides supervisory guidance related to the topic of insurance management:

Advisory Bulletin AB 2014-02, dated February 18, 2014: Operational Risk Management. Provides guidance to the regulated entities on the effective management of operational risk and is intended to promote the safety and soundness of the regulated entities by providing specific guidance upon which each regulated entity should manage operational risks.

6) Advisory Bulletins of the predecessor Federal Housing Finance Board that provide supervisory guidance related to the topic of insurance management:

Advisory Bulletin 02-3, dated February 13, 2002: Disaster Recovery Planning. Provides guidance on specific attributes to be considered by FHLBanks in the formulation of their business continuity plans and the establishment of bilateral agreements with other FHLBanks.

Advisory Bulletin 03-2, dated February 10, 2003: Business Continuation Contingency Planning. Provides guidance on specific attributes to be considered by FHLBanks in the formulation of their business continuity plans and the establishment of bilateral agreements with other FHLBanks.

Advisory Bulletin 05-05, dated May 18, 2005: Risk Management Oversight. Provides guidance on the risk management function, and the risk management responsibilities of the board of directors and senior management.

7) OFHEO Policy Guidance that provides supervisory guidance applicable to the topic of insurance management:

Policy Guidance PG-00-001, December 19, 2000: Minimum Safety and Soundness Requirements. Requires management of the Enterprises to establish and maintain an effective risk management framework, including reviewing such framework to monitor its effectiveness and take appropriate action to correct any weaknesses. OFHEO codified the policy guidance at 12 CFR 1720.

Examination Guidance PG-06-001, November 8, 2006: Examination for Corporate Governance. Sets forth examination guidance and standards relating to the corporate governance of the Enterprises.

8) Other government agencies' and non-government resources pertaining to insurance management:

Federal Financial Institutions Examination Council (FFIEC) IT Examination HandBook – The Business Continuity Planning, Information Security and Management booklets address specific controls and procedures related to insurance management.

Office of the Comptroller of the Currency (OCC); Comptroller's Handbook – Risk Management and Insurance (Section 406), March 1990 addresses the use of insurance for risk management strategies.

Bank for International Settlements (BIS); Basel Committee on Banking Supervision – Principles for the Sound Management of Operational Risk, June 2011, addresses the use of insurance for risk management strategies.

COBIT®; 5 for Risk, 2013, addresses the use of insurance as a tool to respond to risk.

Issues Specific to the Regulated Entities and the Office of Finance

Each board has the ultimate responsibility to ensure its regulated entity or the OF maintains a satisfactory insurance management program. The organizational unit responsible for the management of the insurance program may differ, as it may be assigned to the facilities management, administrative services, accounting, human resources, and/or the legal services functions; however, the board should require updates on any insurance matters that may affect the regulated entity or the OF.

Elements of an effective insurance management program include:

1) Coordination of the insurance management program among the regulated entity's or the OF's key/critical operations such as accounting, credit, collateral, cash management, executive department, funds transfers, investments, community investment services, human resources, safekeeping, document custody operations, financial management, information technology, and legal services, so that the risks presented by each area of operation are adequately addressed in the regulated entity's or the OF's insurance coverages.

2) Ongoing communication with the regulated entity's or the OF's insurance agent/broker. This includes reviewing with such agent/broker periodic surveys and documentation of trends, new issues/developments, and claims histories involving the regulated entity or the OF. The insurance broker should review changes in building plans and major equipment installations. In addition, management should keep its insurance agent/broker aware of changes in the regulated entity's or the OF's risk exposure that might have occurred between insurance review periods.

3) Management must have a sound understanding of changes in the insurance market and of available coverage that may affect the insurance management program. Management should also be aware that independent insurance agents/brokers receive commissions and therefore are financially interested in the sale of insurance policies to the regulated entity or the OF. Consequently, they may not provide fully objective advice regarding insurance needs. Therefore, the regulated entity or the OF should

consider engaging an *independent* insurance consultant to provide a "second opinion" as to the adequacy of insurance coverage.

4) The board's minutes should document its review and approval of the regulated entity's or the OF's insurance management program and insurance coverage. The board may assign a board committee to discuss and provide oversight, but the board itself is ultimately responsible for the insurance management program and to ensure adequate coverage is maintained. Should a board committee be established to oversee the insurance management program, the committee's chair and the responsible management representative should make a presentation to the full board annually.

Examination Workprogram

The workprogram for the Insurance 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 document sufficient worksteps from Section 4, *Testing*, to support the findings and conclusions from this examination module.

In determining the extent of review and testing to be conducted in completing each examination, the examiner should take into account any applicable FHFA off-site monitoring or analysis reports, such as analyses of 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 regulated entity's or the OF's insurance management activities.

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

1. Scope of Examination Work Performed

1) Review past reports of examination for outstanding issues or previous problems related to insurance management. Review workpapers from the most recent examination when the scope included a review of insurance management.

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

3) 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 insurance management.

4) Review internal audit or quality assurance reports for outstanding issues relating to insurance management.

5) Review for and address any applicable portions of FHFA issued Advisory Bulletins or other examination guidance documents.

6) Review minutes of meetings of the board of directors and relevant board and management committees for any issues regarding insurance management.

7) Review management's response to audit recommendations noted since the last examination. *(Was management's response adequate? Was the timing of corrective action appropriate? Did management resolve the root causes of the issues rather than just specific audit deficiencies? Are any issues still outstanding? How effective are any monitoring systems used to track the implementation of recommendations on an on-going basis?)*

8) Interview management and review the insurance management request information to understand the regulated entity's or the OF's insurance management process. *(Have there been any significant changes in management, business strategies, or internal business processes that could affect the insurance management process? What has changed outside of the regulated entity (industry, regulatory environment) since the last examination? Have there been any material changes in the audit program, scope, or schedule related to insurance management activities? Have there been any changes in key insurance providers? Have there been any other internal or external factors that could affect the insurance management process?)*

9) Establish and document the scope of the examination by focusing on those factors that present the greatest degree of risk to the regulated entity or the OF. *(What are the examination objectives? What are the details of what will be reviewed? What will not be reviewed in order to evaluate the regulated entity's insurance management program?)*

Summarize the work performed in the examination of insurance management. 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

1) Determine if since the last examination, the regulated entity or the OF has undergone changes that would expose it to any new or different levels of insurable risk, and/or identified any previously uninsured risks. Determine if the regulated entity or the OF evaluated the potential need for increased or different insurance coverage. *(How effective is the regulated entity's process for identifying new or different insurable risks? Has the regulated entity failed to identify any new insurable risks)*

2) Evaluate the regulated entity's or the OF's analyses of trends in insurable exposures to the organization. *(How effective is the regulated entity's process for identifying and assessing the effects of trends in the risks? Has the regulated entity identified risks that may be mitigated by insurance coverage? Has the regulated entity made sound decisions for which risks to insure against? Are there any trends in the risks that the regulated entity failed to identify?)*

3) Determine if there have been any changes in the industry that would expose the regulated entity or the OF to any new risks, affect the regulated entity's or the OF's exposure to risks, or change the trends of any risks. *(If yes, how effective was the regulated entity's process to identify and assess the effect of the change?)*

4) Determine if the regulated entity or the OF assesses on a reasonably frequent basis, at least annually, the types and degrees of uninsured risks the regulated entity or the OF is willing to assume. *(Is the frequency of the assessment appropriate? Is the quality of the assessment adequate? Is the assessment well documented? Are the assumptions reasonable?)*

5) Determine if the regulated entity or the OF conducts periodic appraisals of major fixed assets to be insured. *(Is the list of major fixed assets appropriate? Are the appraisals appropriate? Are the appraisals well documented?)*

3. Risk Management

Risk Identification Process

1) Determine if the regulated entity or the OF analyzes the credit or financial condition of the insurance companies who have issued policies to the entity. *(Is the analysis appropriate? Is the analysis well documented? Is the analysis timely?)*

2) Determine if the regulated entity or the OF maintains records, by type of risk, to facilitate an analysis of the entity's experience in costs, claims, losses, and settlements under the various insurance policies in force. *(Are the regulated entity's records complete? Is the information recorded in a timely manner?)*

3) Determine if the regulated entity's or the OF's insurance coverage is current. *(If any insurance coverage has lapsed, how long has the regulated entity been without coverage? What steps are being taken to obtain adequate coverage? What was the cause for the lapse in insurance coverage? What changes has the regulated entity implemented to ensure that a similar lapse does not occur again?)*

4) Determine if the entity use the services of a professional, knowledgeable insurance agent or broker to assist in selecting and providing advice on alternative means of providing insurance coverage. *(How effective was the advice provided by the agent or broker? Did the regulated entity also conduct independent analysis to ascertain the best insurance coverage for the entity?)*

5) Determine whether insurance coverage provides adequate protection for the regulated entity or the OF. *(Have there been any losses incurred that were not covered by insurance? Was the regulated entity aware of the risk for the loss before it occurred? If so, was the analysis performed to accept the risk appropriate?)*

Organizational Structure

1) Determine if the regulated entity or the OF has designated a risk manager who is responsible for risk control. *(Are the qualifications for the risk manager appropriate? Does the regulated entity have a process to ensure the risk manager obtains appropriate training in a timely manner? Does the regulated entity provide the risk manager with the proper authority and resources to effectively conduct the assigned responsibilities of a risk manager?)*

2) Determine if the entity has established an Office of Minority and Women Inclusion, or has designated an office of the regulated entity, that is responsible for carrying out all matters of the entity relating to diversity in management, employment, and business activities. *(What is the regulated entity's process to ensure diversity in management, employment, and business activities?)*

Policy and Procedure Development

1) Assess written policies, procedures, and standards pertaining to insurance management. *(Are there appropriate policies, procedures, and standards used to identify and analyze risks? Are they accurate, timely, complete, relevant, and consistent? Is the level of coverage adequate? How appropriate are the methods used to control and treat risks?)*

2) Determine if the board has established appropriate guidelines or thresholds for the maximum risk they are willing to accept. *(How effective are the regulated entity's methods to ensure risks are maintained within these guidelines or thresholds? How appropriate was the board's analysis to identify the guidelines or thresholds they were willing to accept? Have there been any instances where the regulated entity's risk exposure was above the guidelines or thresholds? If so, what steps has the regulated entity taken to ensure a similar occurrence does not happen again?)*

3) Determine if management has established appropriate operating procedures for filing insurance claims. *(Does the regulated entity have an effective process to ensure that it is taking prompt action when fraudulent activity is suspected to avoid further losses after what may later be regarded by the insurer as the date of discovery? Does the regulated entity consider obtaining the advice and assistance of legal counsel, consultants, or accountants in filing claims? Does the regulated entity ensure adherence with insurance policy filing and notification requirements? Does the regulated entity allocate human and monetary resources as warranted by the significance of the claim? Does the regulated entity ensure adequate monitoring and follow-up after the claim is filed?)*

4) Determine if the regulated entity has developed and implemented standards and procedures to ensure, to the maximum extent possible, the inclusion and utilization of minorities and women, and minority- and women-owned businesses in all business and activities of the regulated entity at all levels, including in insurance. *(Are the regulated entity's standards and procedures effective? What types of reports are produced for management? What are the trends in the number of minorities and women included and utilized in all business activities?)*

Risk Metrics

1) Determine if the regulated entity or the OF monitors any metrics pertaining to insurance coverage. *(If yes, how effective are the risk metrics? Are they accurate, timely, complete, relevant, and consistent?)*

Reporting

1) Determine if a complete schedule of insurance coverage is presented to the board, at least annually, for its review. *(Does the board demonstrate their understanding of the risks and the mitigation steps being taken through the discussions documented in the minutes? Is the information presented to the board accurate, timely, complete, relevant, and consistent?)*

Internal/External Audit

1) For internal audits completed since the previous examination addressing insurance management, consult with the Office of the Chief Accountant (OCA) regarding any findings about the adequacy of the scope and testing performed by internal audit.

2) If there are no prior findings, select internal audits related to insurance management and determine whether or not the scope of the audit work 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 compliance with policies? Does the scope include an evaluation of internal controls and testing of operational processes? Do the workpapers include a clear trail to conclusions? Do the workpapers identify areas for further review?)*

3) Coordinate with OCA to determine whether or not external audit performed work on insurance management risk management and whether or not OCA performed an evaluation of the adequacy of the scope and testing completed by external audit.

Information Technology

1) Determine if the regulated entity or the OF maintains a concise, easily referenced summary or schedule of existing insurance coverage. If the regulated entity or the OF does not maintain a schedule, request that management complete a schedule of existing insurance coverage. *(Is the summary or schedule accurate, timely, complete, relevant, and consistent?)*

Compliance

1) Determine if the regulated entity or the OF is in compliance with applicable laws and any pertinent supervisory guidance. *(Are there any instances of violations? If so, what are the root causes of the violations? How should internal controls be strengthened to ensure there are no future regulatory violations?)*

2) Using the insurance coverage summary prepared by the entity, determine whether coverage conforms to the guidelines for maximum loss exposure established by the board. *(Are there any instances where loss exposure is greater than the limits established by the board? Was the regulated entity aware that the loss exposure was greater than the limits established by the board? What changes must take place to ensure that similar loss exposure does not occur again?)*

3) Determine if the regulated entity or the OF is in compliance with all applicable board-approved policies and procedures. *(Are there any instances where the regulated entity is not in compliance with the board-approved policies and procedures? What changes must take place to ensure that similar non-compliance does not occur again?)*

4) Specifically assess the regulated entity's adherence with 12 CFR Part 1236 Prudential Management and Operations Standards (PMOS). In particular:

   a. Standard 1 – Internal Controls and Information Systems

i. Principle 8 – A regulated entity should have an effective risk assessment process that ensures that management recognizes and continually assesses all material risks, including credit risk, market risk, interest rate risk, liquidity risk, and operational risk. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

b. Standard 8 – Overall Risk Management Processes

i. Principle 1 – Regarding overall risk management processes, the board of directors is responsible for overseeing the process, ensuring senior management is appropriately trained and competent, ensuring processes are in place to identify, manage, monitor, and control risk exposures (this function may be delegated to a board appointed committee), approving all major risk limits, and ensuring incentive compensation measures for senior management capture a full range of risks. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

ii. Principle 9 – A regulated entity should have 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. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

4. Testing

1) Complete testing, as appropriate, to assess adherence with the board-approved insurance management program and risk management strategies.

2) Review the regulated entity's or the OF's process for obtaining insurance coverage. Evaluate and conclude on efforts to receive bids for insurance coverage. Determine if the regulated entity or the OF has established appropriate criteria for insurance providers and assess and conclude on the regulated entity's or the OF's efforts to ensure all insurance providers meet the minimum standards established.

3) Select a sample of policies in place for the regulated entity or the OF. Assess and conclude on whether the coverage is comprehensive. *(Is the coverage adequate to cover all potential risks to the regulated entity? Are any restrictions to coverage reasonable?)*

4) If any, select a sample of claims the regulated entity or the OF has made under its insurance program. *(Were claims handled appropriately? Were losses incurred as a*

result of internal control weaknesses within the regulated entity? If losses were a result of weaknesses in internal controls, has the regulated entity taken appropriate steps to address the concerns?)

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 or the OF's insurance management practices. Develop a memorandum describing the risks to the regulated entity or the OF related to insurance and the regulated entity's or the OF'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 regulated entity or the OF is exposed to in the insurance area (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 regulated entity's or the OF's response to previous examination findings and concerns.

3) Develop findings and prepare findings memoranda, as appropriate. Based on examination work performed, develop findings communicating concerns identified during the examination. Findings should identify the most significant risks to the regulated entity or the OF and the potential effect to the regulated entity or the OF resulting from the concerns identified. Such documents should describe a remediation plan specifying the appropriate corrective action to address examination concerns and establish a reasonable deadline for the regulated entity or the OF to remediate the finding. Communicate preliminary findings to the EIC. Discuss findings with regulated entity or OF personnel 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 regulated entity or the OF 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 or the OF's practices or anticipated external changes that could affect the regulated entity's or the OF's future insurance needs.

Workprogram

1. Scope of Examination Work Performed

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

2. Description of Risks

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

3. Risk Management

- Assess and conclude on the adequacy of the regulated entity's or the OF's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
    - The regulated entity's or the OF's organizational structure
    - Policy and procedure development for insurance management
    - 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 in the insurance management area
- Assess and conclude on the adequacy of the regulated entity's or the OF'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 insurance management
    - Conclude on the level of risk to the organization
    - Include an assessment of the adequacy of an regulated entity's or the OF's monitoring of risk and establishment of internal controls to mitigate risk
- Conclude on responsiveness to examination findings from previous examinations
- Develop examination findings, as appropriate
- Identify areas requiring follow-up examination activities or monitoring