FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2016–05

INTERNAL AUDIT GOVERNANCE AND FUNCTION

Purpose

This Advisory Bulletin (AB) applies to Fannie Mae and Freddie Mac (the Enterprises), the Federal Home Loan Banks (FHLBanks) (collectively, the regulated entities), and the FHLBanks' Office of Finance (OF). References to the regulated entities[1] in this AB equally apply to the OF. This AB rescinds and replaces the following guidance:

- 2002-AB-05: *Risk Assessment – Internal Auditor Independence;*
- 1999-AB-10: *Internal Audit Department External Reviews;* and
- 1996-AB-01: *Examination Reviews of Audit Independence, Audit Committee Oversight of Selection, Compensation and Performance Evaluation of the Audit Director*.

The Federal Housing Finance Agency (FHFA) requires the regulated entities to establish independent Internal Audit (IA) functions and expects those IA functions to provide timely feedback to management and assurance to audit committees on the effectiveness of regulated entities' internal controls, risk management, and governance. Timely and reliable information about elevated risks and internal control systems are important so that management can make prompt corrections. This AB sets forth FHFA guidance and supervisory expectations regarding:

I. Audit Committee Oversight of the IA Function;
II. IA Independence and Objectivity; and

[1] The OF is not a "regulated entity" as the term is defined in the Federal Housing Enterprises Financial Safety and Soundness Act as amended. However, for convenience, references to the "regulated entities" in this AB should be read to also apply to the OF.

III. IA Attributes and Operations - including IA's role in reporting to the audit committee on the regulated entity's identification of significant risks and the existence and effectiveness of related internal controls.

A regulated entity's risk management framework generally comprises:

- Units engaged in business operations, which take and manage risks and report directly to management;[2]
- Independent risk management (including enterprise risk management, compliance, and other risk control functions), which monitors risk-taking activities, assesses risks and issues independent of business operations units, and is separate from first-line operating management but still under the direction and control of senior management; and
- IA, which reports independently to the audit committee on risks, risk management, and the effectiveness of the regulated entity's system of internal controls.

This structure is commonly known as the "three lines of defense," and together these elements should form a strong and effective risk management framework. The guidance in this AB is consistent with the three lines of defense framework and sets forth FHFA's expectation that IA, as the third line of defense, is independent, objective, and effective at identifying and informing management and the audit committee about the regulated entity's risks and related controls.

FHFA expects Chief Audit Executives (CAEs)[3] to establish and audit committees to oversee IA functions that:

- Are independent and objective;
- Continuously monitor key activities and associated risks;
- Adapt audit approaches and activities to address changes; and
- Identify and communicate internal control deficiencies and emerging, previously unidentified, or undervalued risks (*i.e.*, risks that have become more significant) to the audit committee and management.

FHFA further expects audit committees, through their direction to and oversight of CAEs and IA functions, to validate that staffing and resource decisions take appropriate account of the risks at the regulated entity. FHFA expects that these decisions consider the entity's size, scale, complexity of operations, pace of innovation, and financial standing.

[2] "Management" as the term is used in this guidance generally comprises the CEO and subordinate managers, who engage in business operations.
[3] As used in this guidance, the term "Chief Audit Executive" means the individual responsible for the internal audit function at a regulated entity.

Background

FHFA recently published a revised rule, 12 CFR Parts 1236 and 1239, *Responsibilities of Boards of Directors, Corporate Practices, and Corporate Governance Matters*, that in part addresses regulated entities' audit committees' oversight of IA functions at the FHLBanks and the Enterprises. In addition, FHFA's standards for the FHLBanks and Enterprises specifically related to their audit committees and IA functions are in Standard 2 of the *FHFA Prudential Management and Operations Standards* (PMOS) (12 CFR Part 1236, Appendix). FHFA requirements relating to the OF's audit committee are set forth at 12 CFR 1273.9.

For the FHLBanks, the regulations prescribe specific details about the composition of the audit committee, the independence of its members, the content of the audit committee charter, and the duties and responsibilities of the audit committee, including its oversight responsibilities with respect to the IA function.[4]

The OF is the FHLBanks' fiscal agent. It compiles and publishes the FHLBanks' Combined Financial Reports. The OF's audit committee composition, responsibilities, and charter are addressed in 12 CFR 1273.9 and are similar to those applicable to FHLBanks. The OF is not a Securities and Exchange Commission registrant.

For the Enterprises, regulations in 12 CFR 1239.5(b) require that all the board committees comply with requirements established by the New York Stock Exchange (NYSE) and that the audit committees also comply with the requirements of Section 301 of the Sarbanes-Oxley Act of 2002.[5] Relevant portions of the NYSE rules address the composition of the audit committee, the independence of its members, the general requirements for its charter, the responsibilities and duties of the audit committee (which include assisting the board in oversight of the IA function), and the need for audit committees to meet separately and periodically with management, CAEs, and independent auditors.[6]

Because the existing regulations and guidelines provide general requirements for oversight of the IA function, FHFA is issuing this AB to provide an additional level of detail on the responsibilities of audit committees in their oversight of the IA function, as well as on the independence and operation of the IA function. This guidance reflects FHFA's supervisory expectations that the audit committee actively and rigorously oversees the IA function and that the function is independent, objective, and effective. Further, this guidance is informed by FHFA's understanding of industry best practices for IA governance and operations at larger and more complex financial institutions.

[4] 12 CFR 1239.32.
[5] Section 301 of the Sarbanes-Oxley Act does not directly address the audit committee's oversight of the IA function.
[6] NYSE Listed Company Manual, Rule 303A.07.

In addition, the provisions of this AB are consistent with IA guidance issued by the federal banking regulatory agencies. That guidance includes the *Interagency Policy Statement on the Internal Audit Function and its Outsourcing* (March 17, 2003) and the Federal Reserve Board's *Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing* (January 23, 2013). This AB is also consistent with the *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR Parts 30 and 170* (effective November 10, 2014) and with guidance in the October 27, 2009 FHFA *Examination for Accounting Practices* document, which remains in effect.

Guidance

I. Audit Committee Oversight of the IA Function

The board of directors of each regulated entity is required to have an audit committee responsible for overseeing the IA function and an individual responsible for the IA function (referred to in this document as the CAE, regardless of that individual's title). The audit committee should have regular and open communications with the CAE.

The audit committee should direct the CAE to structure the IA function so that it is appropriately designed, independent, and objective, and so that it effectively identifies and assesses risks. The committee should confirm that the regulated entity's IA audit methodology is established and activities are conducted in accordance with appropriate professional standards, such as the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing (IIA Standards).* The CAE should periodically review IA's audit methodology with the committee and the committee should approve the methodology and significant changes thereto. Further, the audit committee should oversee the process by which issues that are reported by IA are promptly addressed and satisfactorily resolved by management.

A. *Audit Committee Charter and the Internal Audit Function*

The audit committee is required to operate pursuant to a written charter,[7] which should be reviewed at least annually by the audit committee and full board of directors (board), and be re-approved at least every three years by the board.[8]

FHFA expects that, at a minimum, the audit committee charter will address the following matters

[7] 12 CFR 1239.5(c).
[8] For the FHLBanks, annual review by the committee and the full board, and re-approval by the board at least every three years are required by regulation. 12 CFR 1239.32(d).

regarding the IA function:[9]

- CAE selection, evaluation, compensation, and where appropriate, replacement: The charter should establish that the CAE may be hired or removed only with audit committee approval.
- CAE reporting relationships: The charter should establish that the CAE reports directly to the audit committee and is ultimately accountable to the audit committee and board of directors in order to maintain independence and objectivity.
- CAE access to the audit committee: The charter should provide the CAE with unrestricted access to the committee without the need for any prior management knowledge or approval and should establish executive session meetings with the CAE.
- Annual review and approval of the Audit Plan: The committee should confirm that the scope of IA's activities is appropriate and approve the annual Audit Plan and significant changes thereto.
- Annual review and approval of the IA department's budget: The committee should confirm that IA has sufficient resources to accomplish its objectives and approve the department's budget.

B. *Audit Committee Communication with Internal Audit*

The audit committee and the CAE, including IA staff, should have unrestricted access to each other without prior management knowledge or approval. FHFA expects audit committee leadership to discuss audit matters with the CAE between and apart from regular audit committee meetings to stay current on IA operations, emerging risks, and other relevant matters. If significant issues arise in these discussions, they should be covered timely with the committee. Regular executive sessions with the CAE are essential to ensure open and complete communications. These executive sessions should be confidential, closed to management, and should be regularly scheduled.

An important component of effective communications between the CAE and audit committee are the regular written reports to the audit committee prior to each meeting and otherwise as warranted. Regular written reports from IA to the committee should generally address:

- Audit Findings and Risk Analyses:
    - Audit reports focusing on less than satisfactory findings;
    - Significant and higher-risk issue follow-up information, including potential impact, aging, past-due status, root-cause analysis, progress towards remediating significant findings, and thematic trends;

[9] For the FHLBanks, these items, except audit committee approval of IA department budget approval, are regulatory requirements. 12 CFR 1239.32(d) (3), (e) (3).

- Clear, timely, detailed reporting on open remediation plans, along with associated timetables that were agreed upon by stakeholders for significant open audit issues;
- Information on significant industry and institution trends in risks and controls;
- An assessment of risk management processes, including whether monitoring processes are appropriate and the effectiveness of management's self-assessment and remediation of identified issues; and
- Aggregate information on the nature of significant trends, if any, in audit findings and observations that have been communicated to management but not detailed in reports to the audit committee.

- Audit Department Performance and Processes:
  - Audit coverage and completion versus the Audit Plan;
  - Budgeted versus actual audit hours;
  - Any updates or amendments to the Audit Plan, including support for changes;
  - Results of internal and external quality assurance reviews;
  - Updates on the status of IA annual goals and objectives;
  - Significant changes in audit staffing levels and the status of required staff training;
  - Information on major projects and initiatives; and
  - Any significant changes in IA processes, including a periodic review of key IA policies and procedures.

C. *Monitoring and Performance Assessments*

The audit committee should maintain a robust process for monitoring and, at least annually, formally assessing and evaluating CAE performance and the effectiveness of the IA function. The process should generally incorporate input from senior management and external auditors, from any outside peer reviews or assessments including regulatory examinations, and from the audit committee's own observations of and interactions with the CAE and IA staff. The audit committee should document its assessments of the CAE's and IA function's performance.

II. IA Independence and Objectivity

A. *Conflicts of Interest*

Before appointing a CAE, and thereafter at least annually, the audit committee should confirm with the CAE and document whether the CAE has any actual or apparent conflicts of interest and should develop appropriate limits for the CAE's activities accordingly. If an audit committee considers a candidate for CAE with potential conflicts of interest, the conflicts, and any mitigating considerations, should be disclosed to and discussed by the audit committee and should be clearly documented in audit committee records.

Similarly, the CAE should regularly assess whether IA staff has actual, potential, or apparent conflicts of interest and appropriately restrict the activities of the staff to avoid those conflicts. At least annually, the CAE should confirm IA activities' independence to the audit committee. To help maintain the highest level of objectivity in the IA function, CAEs should consider rotating assignments for lead auditors and audit staff when feasible.

B. *Placement of IA in the Organization*

Properly positioning the CAE and the IA function in a regulated entity's organization helps achieve objectivity and independence of the IA function and minimizes the opportunity for management to unduly influence, override, or limit IA activities or findings. The most structurally independent organizational arrangement for the IA function would have the CAE report directly to the audit committee regarding both audit issues and administrative matters. However, the CAE may report administratively to the Chief Executive Officer (CEO) if the audit committee so approves.[10]

Board and senior management engagement and cooperation with IA are essential to its effectiveness. Boards and management should give IA full and unconditional access to any records and data, including access to management information systems and records and the minutes of all board and management committee meetings. FHFA expects IA to have access to management committee meetings and related materials in an ex-officio capacity, and any exceptions should be discussed and reconciled with the audit committee. Boards and management should also require timely remediation of audit issues.

C. *Scope Limitations*

Should management attempt to hinder IA's objectivity and independence, for example, by restricting IA's access to records or personnel, IA staff should disclose to and discuss such attempts with the CAE. If the scope of an audit is affected by management's action, the limitation should be disclosed in the audit report and documented in the associated work papers. The CAE should report any attempts to hinder IA's objectivity and independence or limit the scope of an audit activity to the audit committee, generally through the chair, immediately for appropriate resolution.

D. *Internal Audit Compensation Arrangements*

CAE compensation, which should be approved by the audit committee, should include an

[10] 12 CFR Part 1273.9 (b) (5), which relates to the OF only, states "the internal auditor shall report directly to the Audit Committee and administratively to executive management."

appropriate focus on performing audit activities and should only include incentives tied to actions and outcomes within the CAE's control and influence. Audit committees should not link CAE incentive compensation to the regulated entity's financial position, results of operations, achieving growth or volume targets, business unit compliance levels, or other measures or metrics that could impair or appear to impair IA independence or objectivity. CAE compensation should be reasonable and comparable with compensation for employment in other similar businesses (including publicly held financial institutions or major financial services companies) involving similar duties and responsibilities. To these ends, consulting with and obtaining input from a regulated entity's compensation committee may provide useful insights.

III. IA Attributes and Operations

A. *IA Function Attributes*

1. *Internal Audit Department Charter*

The IA department should have a written charter, which should be reviewed at least annually and be approved by the audit committee every three years or whenever substantive changes are made. The charter should define the purposes, authorities, and responsibilities of the IA function. The charter is the foundational document governing all IA activities. The charter should generally cover:

- IA Department Structure and Independence
    - Indicate the IA function's placement within the regulated entity, the CAE's and IA function's authority, the CAE's functional reporting relationship to the audit committee, and the CAE's administrative reporting to senior management, if any;
    - Stipulate that IA has unrestricted access to the audit committee and authorize staff to access all regulated entity records and personnel needed to carry out their function; and
    - Require the IA function to maintain its independence and objectivity, particularly if IA provides non-attest services, such as consulting on internal controls design for information technology projects, performing financial reporting internal controls testing under management direction, and/or identifying potential operating inefficiencies for management.
- Applicable Standards and Codes of Ethics
    - Identify standards applicable to the IA function and staff, including any professional standards, such as the Institute of Internal Auditors (IIA) Standards; and
    - Identify codes of ethics and requirements with which IA staff must comply. These may include both the regulated entity's own written code and one or more professional standard codes, such as the IIA's Code of Ethics.

- Reporting
    - Indicate regular reports and items that the IA function is required to provide to the audit committee, including audit plans and annual budget and resource requirements;
    - Require timely reporting of significant deviations from approved plans; and
    - Require the IA function to monitor and report its activities and management's responses to IA findings, and track, assess, and regularly report on management's remedial actions regarding significant open compliance and regulatory examination issues.
- Performance Assessment and Quality Assurance
    - Require the IA function to regularly assess its performance, including its performance relative to the Audit Plan;
    - Require the IA function to maintain internal quality assurance processes and programs, and document how weaknesses identified as a result of such processes and programs are addressed; and
    - Establish the timeframe for regular external quality reviews (at a minimum every five years) and require the IA function to document how any weaknesses, recommendations, or best practice suggestions identified as a result of such external quality reviews are addressed.

2. *IA Staffing and Professional Competence*

The IA function needs sufficient staff with the requisite knowledge, skills, professional competence, resources, and stature within the regulated entity to assess the effectiveness of the regulated entity's controls and to credibly challenge management.

A regulated entity should have policies and procedures designed to reinforce that:

- The IA function hires and maintains sufficient, technically competent staff to provide adequate audit coverage of the regulated entity's risks;
- IA staff are provided appropriate training and professional development opportunities to enable them to remain current in both technical matters and professional standards; and
- IA staff understand their duties, including the duty to report instances of non-compliance with laws, regulations, regulatory guidance, generally accepted accounting principles, professional standards, or the regulated entity's own policies to the CAE, management, and/or the audit committee, as appropriate.

Collectively, IA staff, supplemented as needed by external resources, should have the knowledge and skills, as evidenced by education and audit, industry, and technical experience, to audit the entire regulated entity. Relevant and current professional certifications and licenses provide evidence of certain technical knowledge and skills. Generally, IA staff should audit

business units or functions related to their areas of expertise.

At least annually, the CAE is expected to assess and document the knowledge, skills, and abilities of IA staff and compare those with both the Audit Plan and the universe of risks in the regulated entity. When assessing the knowledge, skills, and abilities of IA staff, the CAE may consider management feedback and internal or external quality assurance assessments. If the assessment identifies gaps within IA staff knowledge, skill, and abilities, the CAE should identify a means for filling those gaps, which might include staff training, hiring new staff, and/or using co-sourcing or outsourcing arrangements. The CAE should report the results of the assessment to the audit committee.

The CAE should confirm that he/she and all IA staff receive ongoing formal training. CAEs and staff should generally receive a minimum of forty hours of training per year. The IA function should have a process to evaluate and monitor the quality and appropriateness of training. In addition to formal training, IA staff may benefit from staff rotations, both within the IA department and with business and risk management functions, in order to provide IA staff with broader exposure to those functions and opportunities to develop additional areas of expertise. We encourage such rotations where they are feasible and can be done without compromising audit coverage and IA independence.

3. *Co-sourcing and Outsourcing Internal Audit Activities*

The IA function may be staffed using IA employees solely or by supplementing them with co-sourced or outsourced resources.[11] Co-sourcing or outsourcing engagements are generally entered into when a regulated entity has insufficient staff to complete planned audits in a timely manner or needs technical expertise beyond that of the IA staff. The CAE retains responsibility for managing and providing the audit committee with reports to enable the audit committee to oversee all IA work, whether done by IA staff, co-sourced, or outsourced.

Co-sourcing is a partnership between IA and an outside vendor (auditor or firm) that works with and often alongside, but does not replace, existing IA staff. In co-sourcing, IA staff takes an active part in project planning and decision making and may participate in preparing final reports. Further, IA manages and/or works alongside the specially-skilled partner(s) or vendor(s). One objective of co-sourcing may be to transfer knowledge from the vendor to IA. In a co-sourcing arrangement, the vendor has a dual reporting relationship to IA and the vendor's own management. The CAE should require in associated contracts with co-sourced partners that work complies with applicable IA policies and standards and that the workpapers associated with

[11] Co-sourced and outsourced audit engagements should be awarded in compliance with the requirements for equal opportunity in employment and contracting under applicable provisions of the Minority and Women Inclusion and Diversity at Regulated Entities and the Office of Finance regulation, 12 CFR 1207.21.

the co-sourced work are retained by IA, not the vendor.

Under an outsourcing arrangement, the outside vendor (auditor or firm) is responsible for performing discrete IA engagements. The CAE maintains ownership of the entire IA function, including outsourced activities. When outsourcing audit work, the CAE should approve the scope of work and procedures to be performed. The CAE remains responsible for results of outsourced work, including findings, conclusions, and recommendations.

Before hiring a vendor to perform IA work, the CAE should confirm that: the vendor and staff who will work on the engagement have the technical knowledge and ability to perform the work; the engagement will be effectively managed; the vendor's work will be well-documented; that all control weaknesses and other significant findings, including any apparent regulatory violations, will be timely communicated to the CAE and other stakeholders; and that the regulated entity has appropriate contingency plans should a vendor be released or terminated before completing the engagement.

Co-sourced and outsourced audit work should be completed pursuant to an engagement letter or similar agreement covering all significant aspects of the engagement. Such engagement letters should generally:

- Describe expectations and responsibilities for the regulated entity and the vendor;
- Define the work to be performed and the amount and timing of fees to be paid;
- Describe the responsibilities for providing and receiving information, including the type and frequency of contract work status reporting to the CAE and the audit committee;
- Describe the process for changing engagement terms, such as for expanding work if significant issues are identified;
- Define conditions that would constitute default and remedies including canceling the engagement;
- Establish who bears the cost of damages arising from errors, omissions, and negligence;
- State that the vendor will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of management or an employee and, if applicable, will comply with American Institute of Certified Public Accountants, Securities and Exchange Commission, Public Company Accounting Oversight Board, and other relevant professional standards, and other applicable regulatory guidance; and
- For any engagements where reports or workpapers will be retained by the vendor:
    - Establish that reports created by the vendor during the engagement are the property of the regulated entity, that the regulated entity will be provided with any copies of the related workpapers it deems necessary, and that employees authorized by the regulated entity will have reasonable and timely access to the workpapers prepared by

the vendor;
- Specify the locations of reports and the related workpapers and the length of time vendors must maintain workpapers;
- State that FHFA examination staff will have full and timely access to vendor-created IA reports and related workpapers.

B. *Internal Audit Operations*

1. *Internal Audit Risk Assessments*

Regulated entities' IA universes (comprising all auditable entities[12] that are significant and subject to risks for which controls should be reviewed) should be regularly updated for organizational changes. Audit plans should be formulated to provide reasonable assurance that a regulated entity's system of controls is well-designed, operates effectively, and manages risks to an acceptable level. At least annually, IA should perform a risk assessment that includes reviews of its IA universe and Audit Plan to ensure that all auditable entities receive audit coverage over an appropriate period of time commensurate with associated risks.

The IA risk assessment should include four basic steps: 1) identify inherent risks to the regulated entity; 2) understand management's controls over those inherent risks; 3) assess residual or remaining risks to establish the frequency with which activities should be audited; and 4) prioritize auditable entities from the audit universe for audit coverage. The IA risk assessment should also consider multiple approaches. For example a "top-down" approach could complement a bottom-up approach. A top-down approach begins with identifying industry, environmental, and other enterprise-wide current or emerging risks. A bottom-up approach starts with the audit universe, then assesses and aggregates risks attributable to auditable entities within the audit universe.

The CAE should perform the risk assessment annually and should document the IA staff's understanding of the entity's significant business activities and the associated risks. To facilitate risk assessment and audit planning, IA should maintain (or regularly review if such an inventory is maintained by independent risk management) a complete inventory of all of the regulated entity's material processes, product lines, services, and functions, and then assess the risks, including emerging risks, associated with each. The risk assessment should consider and address risks to the regulated entity from all sources, both internal and external. These include, but are not limited to, credit, market, operational, governance, reputational, fraud, and compliance risk. The assessment should also consider thematic control issues and layered or aggregated risks that

[12] Auditable entities collectively comprise the potential audit universe and may represent business units, departments, processes, general ledger accounts, or other functions at a regulated entity that are suitable for audit.

cross business units or lines of business. The risk assessment should analyze and prioritize key risks and risk management functions.

While the risk assessment should reflect IA's independent analysis, IA may consider all available information, for example, input from management self-assessments. While the formal risk assessment is performed annually, IA should update it as needed for major organizational changes, infrastructure changes, or changes in the regulated entity's external business or regulatory environment.

As underlying technology has advanced, more business entities are using "Continuous Monitoring" (CM) tools to continuously assess and provide management feedback on whether business processes are performing effectively and "Continuous Auditing" (CA) tools, which allow IA to gather and review control-related business process data.

FHFA expects IA functions to employ formal CA and/or CM practices. CA and CM can be conducted by IA staff and/or through technological tools. In either case, it should be done pursuant to written policies and procedures that support consistent and comparable results. CA and CM should be documented through business metrics, management reporting, reports to audit committees, and through any related adjustments made to audit risk assessments and plans. IA should continuously monitor key business metrics and performance indicators. IA should work to understand changes and their drivers in order to help identify potential audit issues and changes in the business environment and to adjust risk assessments and audit plans, if needed, in a timely manner.

2. *Internal Audit Planning*

At least annually, IA should review and update the Audit Plan. The Audit Plan should be based on the risk assessment and should consider key risks and related controls within each significant business and functional activity, the timing and frequency of planned IA work, and a resource budget. During the planning process, IA should analyze the regulated entity's specific risks, mitigating controls, and level of residual risk. The CAE should have a contingency plan to mitigate any significant disruption to audit coverage, particularly for high-risk areas. Documentation supporting the Audit Plan should reference the IA program that describes the objectives of the audit work and the audit work expected to be performed during each IA activity.

The audit planning process should include evaluating management's root cause and lessons learned analyses performed after a significant adverse event. IA should consider management's analysis of reasons for the adverse event and whether it resulted from a control breakdown or failure. IA should confirm that management correctly identified the measures needed to prevent

a similar event from occurring in the future. In certain situations, IA should conduct its own lessons learned analysis outlining the remediation procedures necessary to detect, correct, and/or prevent future internal control breakdowns (including improvements in IA processes).

The audit planning process should also be designed to inform the board's responsibilities for risk oversight to include: overseeing the regulated entity's operational and risk management; remaining informed about the regulated entity's operations and condition; and remaining informed about the entity's risk exposures and senior management's actions to address them. The Audit Plan should be designed to provide the audit committee with the depth and breadth of IA assurance it needs to inform those responsibilities.

3. *Internal Audit Coverage of Risk Management and Regulatory Compliance Programs*

FHFA regulations require the Enterprises and FHLBanks to appoint a Chief Risk Officer (CRO) to implement and maintain appropriate enterprise-wide risk management practices and a Compliance Officer (CO) to head a compliance program designed to assure that they comply with applicable laws, rules, regulations, and internal controls. Both officers should regularly report to the board (in addition, the CRO reports to the Risk Committee) and to the CEO. These functions are part of the regulated entity's second line of defense, its independent risk management function, and are separate from first-line operating management but still under the direction and control of senior management.

IA is the regulated entity's third line of defense. IA should, through its risk assessment and auditing processes, provide the audit committee with independent assurance that enterprise risk management and compliance programs are working effectively, that those programs have identified and reported timely enterprise and compliance risks, and that significant risks are managed to an acceptable level.

4. *Internal Audit Frequency*

Internal audits should generally cover the entire audit universe over a maximum four year period. High-risk areas should generally be audited annually, and moderate- and low-risk audits should be scheduled every 12 to 48 months (or one to four years) based on a risk assessment and ranking that is regularly reviewed and updated. FHFA expects that IA will weigh both inherent and residual risk when deciding on how frequently to audit an area and in considering the audit approach, including the nature and extent of testing. The CAE should confirm that higher level risks, including thematic trends and control issues, are not underreported due to being separately captured in moderate- or low-risk audits.[13] Audit plans should be dynamic and include time to

[13] For example, if a regulated entity relies on user-developed spreadsheets across its operations, and IA has

expand audit work when unexpected or higher risks are identified through CM activities, scheduled audits, or otherwise. The CAE should regularly report significant changes to the audit universe or audit plans to the audit committee, along with an analysis supporting the changes.

5. *Internal Audit Reports*

IA reports should generally present the purpose, scope, objectives, and results of the audit, including findings, conclusions, observations, and/or recommendations however styled. Final reports should also document management's response to findings. IA should maintain work papers that document the work performed and support the audit report.

IA should establish and implement a documented methodology that employs appropriate criteria to prioritize and rank audit issues. The criteria should be sufficiently objective to promote consistent application of judgment and appropriate prioritization of audit issue severity.

6. *Internal Audit Issues Monitoring and Tracking*

Audit committees should regularly receive clear, timely, and detailed reports on significant open violations, findings, weaknesses, and other issues, regardless of their original source. Issues that FHFA requires to be reported to audit committee chairs, whether by FHFA or regulated entities' management, including all FHFA Matters Requiring Attention (MRAs), should be presumed significant. Issues may originate from IA audits and reviews, external audit, regulatory examinations, management self-identification, outside consultants' work, and other sources. IA should also verify that significant risks and/or control deficiencies identified by first- and second-line of defense units, external auditors, or other parties are adequately assessed and communicated to management and board stakeholders. To facilitate the timely and effective remediation of open audit issues, IA and management or the board (as warranted) should agree on a resolution date and on interim milestones, if appropriate.

IA should establish standards for performing timely and appropriately rigorous validation work once management asserts that remediation of significant audit issues (to include MRAs) has occurred. When management or the board indicates that they have performed the required remediation, IA should validate that revised processes and controls are in place, operating, and sustainable before closing the issue. The level of validation work that IA should perform to close an issue will vary based on the issue's risk, complexity, and associated interdependencies. For higher-risk issues, IA should verify that sufficient testing is performed over an appropriate period of time to validate that the issue is sustainably resolved.

---

identified high level or thematic control issues regarding such spreadsheets, the incremental spreadsheet control risk in moderate- or low-risk auditable entities should be aggregated, addressed, and reported appropriately.

IA reports should include key information about open remediation plans and associated timetables agreed on by stakeholders. Reports should highlight significant issues with delayed remediation, including those for which management has made agreed-upon corrective steps and/or control design changes that are pending validation, until testing is complete. These steps should help to verify that control changes are effective and sustainable and to identify issues for which the planned remediation may need to be amended.

Regulated entities should establish and implement policies and/or procedures as appropriate for documenting, monitoring, tracking, and reporting on management's acceptance of risks for any management decision not to remediate audit issues, or for time extensions to perform agreed-upon remediation. If such accepted risks are individually or in aggregate more than insignificant, the CAE should consult with senior management and the audit committee as appropriate.

7. *Quality Assurance Program*

An effective IA Quality Assurance Program (QAP) should be implemented to help minimize audit risk, including the risk that an audit reaches inaccurate conclusions. A QAP should include regular internal processes and reviews, as well as an external Quality Assurance Review (QAR) to be performed at least every five years.

The internal QAP review should include rigorous reviews by IA management and/or peer reviews of reports and work papers for clarity, adherence to IA policies and procedures, and consistency with relevant professional standards. The QAP should help confirm that IA policies, procedures, and processes comply with applicable regulatory and industry guidance; are appropriate for the size, complexity, and risk profile of the regulated entity; are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry; and are followed consistently. QAP reviews and self-assessments may be activity driven or ongoing. Gaps identified should be documented and addressed timely. The CAE should report the results of the QAP to the audit committee at least annually and results from the QAR and any other external review, as received.

Advisory bulletins communicate guidance to FHFA supervision staff and the regulated entities on specific supervisory matters pertaining to the Federal Home Loan Banks, the Office of Finance, Fannie Mae, and Freddie Mac. This Advisory Bulletin is effective January 1, 2017. Contact David R. Poston, Deputy Chief Accountant, Office of Chief Accountant at David.Poston@fhfa.gov or 202-649-3467, or Nicholas J. Satriano, Chief Accountant, at Nicholas.Satriano@fhfa.gov or 202-649-3450, with comments or questions pertaining to this bulletin.