Introduction

Federal Housing Finance Agency (FHFA) staff should understand the principles of sound internal and external audit in order to assess to what extent they can rely on these functions when examining operations of Fannie Mae, Freddie Mac, the Federal Home Loan Banks (FHLBanks), and the Office of Finance (OF) (unless otherwise noted, this module refers to them collectively as the regulated entities).

Each regulated entity must design and implement internal and external audit programs that conform with FHFA regulations and policy, and with professional standards. Examiners should refer to the Regulatory Environment section of this module for FHFA regulations and policy. The scale and scope of the regulated entity's internal audit and external audit program will depend on the entity's size, complexity, scope of activities, and risk profile. While the audit programs may be similar from one regulated entity to another, they should be appropriate for the unique characteristics of each entity. A risk-based internal audit program must include a well-defined risk assessment process that considers all relevant factors and minimizes subjectivity by establishing clear guidelines. The guidelines should define the logical basis for assigning risk grades and risk weights. The guidelines also should have specific criteria for the risk grades (or range of grades) in order to promote consistency and provide a control over the integrity of the risk assessment.

Internal Audit

Internal audit, as defined by the Institute of Internal Auditors (IIA), is "an independent, objective assurance and consulting activity designed to add value and improve the organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." As required by the New York Stock Exchange (NYSE) and the Securities and Exchange Commission (SEC), publicly-traded companies must maintain an internal audit function to provide management and the audit committee of the board of directors with ongoing assessments of the company's risk management processes and system of internal controls.[1] The internal audit function has a broad scope and assesses topics such as the effectiveness of the organization's operations, the reliability of financial reporting, fraud prevention and detection, safeguarding assets, and compliance with laws and regulations.

The internal audit function should serve as a valuable resource for management, the board of directors, and the audit committee of the board of directors by providing an

[1] Fannie Mae and Freddie Mac must comply with NYSE rules. While the FHLBanks are not publicly traded companies, the Housing and Economic Recovery Act of 2008 (HERA) amended the Securities Exchange Act of 1934 (the Exchange Act) to require each FHLBank to register with the SEC under section 12(g) of the Exchange Act. As a result, each FHLBank must comply with the applicable rules issued by the SEC, including audit committee rules.

evaluation of the effectiveness of the regulated entity's operations, risk management, internal controls, and governance. A competent auditor's objectivity, skills, and knowledge can help improve an organization's internal control, risk management, and governance processes. An effective internal audit function also provides assurance to other stakeholders such as shareholders, employees, and regulators.

It is critical that the internal audit function be independent from the entity's business operations. To ensure independence, the internal audit function should report directly to the audit committee of the board of directors and administratively to the most senior executive of the organization — usually the chief executive officer.

While differences amongst the regulated entities may affect the scope and nature of their internal audit practices, each should comply with the IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*). The IIA is an international professional association that provides internal audit professionals with authoritative guidance organized in the International Professional Practices Framework as ***mandatory*** and ***strongly recommended*** guidance. The three mandatory elements are the definition of internal auditing, the code of ethics, and the *Standards*. These standards are required best practices by audit committees and external audit firms, and provide benchmarks to help assess if internal auditors are meeting their responsibilities. Should internal auditors be prohibited by laws or regulations from complying with certain parts of the *Standards*, they should comply with all other parts and make appropriate disclosures.

Internal auditors' responsibilities are generally broader than those of external auditors. External auditors are primarily concerned with the internal control structure relevant to a financial statement audit, which includes an evaluation of the institution's ability to record, process, summarize, and report financial data consistent with the assertions in the financial statements. In addition to these areas, internal audit is also concerned with controls over processes that do not relate to a financial statement audit. Internal audit may conduct regular testing of internal controls to support management assertions regarding the entity's financial statements as required under the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley). If this is the case, however, internal auditors must establish and maintain strict firewalls to prevent auditors from reviewing their own previous work.

External Audit

An external audit program encompasses engaging an independent public accountant to perform a full-scope financial statement audit, a balance-sheet-only audit, an attestation of internal controls over financial reporting, and other agreed-upon external audit procedures.

The external audit provides the board of directors and management with an independent and objective view of activities, including processes relative to financial reporting. An effective external audit function provides reasonable assurance about the effectiveness of internal controls over financial reporting, the accuracy in recording transactions, as well

as the accuracy and completeness of financial and regulatory reports and related disclosures.

Audit Committee

The audit committee serves to, among other things, promote external and internal audit independence and objectivity. The audit committee is responsible for assisting the Board in fulfilling its oversight responsibilities related to the integrity of the financial statements, compliance with legal and regulatory requirements, and oversight of the internal audit function. Generally, the audit committee's responsibility is to act on behalf of the board of directors to ensure that:

1) Financial statements and disclosures are reliable;
2) Internal control and risk management systems are effective;
3) Management and employees comply with the institution's code of business conduct and legal and regulatory requirements;
4) External auditors are independent and qualified and perform adequately; and
5) Internal auditors are objective and perform adequately.

Recognizing the specialized duties and need for independence of audit committee members, regulators and standards-setters have established requirements for entities to establish independent audit committees, to include "financial experts," that audit committees have access to legal counsel, and to establish confidential "whistleblower" access to the committee for employees of public companies and others.

Audit Committee Charter

The audit committee must adopt a formal written charter that details its specific authorities, duties, and responsibilities, including, but not limited to, the following:

1) Committee composition, membership, terms of service, independence, qualifications, and meetings.

2) Reviewing and approving the audit committee charter every three years.

3) Monitoring and/or overseeing the efforts of senior management to maintain the reliability and integrity of the accounting policies and financial reporting and disclosure practices of the regulated entity.

4) Reviewing the basis for the regulated entities' financial statements, the external auditor's opinion on those statements and internal controls, and recommending to the board that the audited financial statements be included in the annual report.

5) Monitoring and/or overseeing the internal audit function by:

a) Selecting, evaluating, and, where appropriate, replacing the audit director and ensuring that the audit director can be removed only with the approval of the audit committee.
b) Requiring that the audit director report directly to the audit committee on substantive matters, and that the audit director shall be accountable to the audit committee and board of directors.
c) Requiring that both the internal and external auditors have unrestricted access to the audit committee without the need for any prior management knowledge or approval.
d) Reviewing the scope of audit services required, significant accounting policies, significant risks and exposures, audit activities, and findings.
e) Monitoring the adequacy and timeliness of internal audit follow-up on business line responses to findings.
f) Assessing the performance and determining the compensation of the audit director.
g) Reviewing and approving the audit director's work plan.
h) Ensuring that the audit committee regularly meets in executive session with both internal and external auditors.
i) Reviewing and approving the internal audit department budget.

6) Monitoring and/or overseeing the external audit function by:

   a) Approving the external auditor's annual engagement letter.
   b) Reviewing the performance of the external auditor.
   c) Making recommendations to the board of directors regarding the appointment, renewal, or termination of the external auditor.

7) Assuring that the internal audit function staff is competent and receives adequate training.

8) Providing an independent, direct channel of communication between the board of directors and internal and external auditors.

9) Determining the extent to which internal and external auditors review the security for computer systems, facilities, and backup systems.

10) Evaluating responses by management to audit findings and reports, and monitoring management's implementation of audit recommendations.

11) Conducting or authorizing investigations into any matters within the audit committee's scope of responsibilities.

12) Monitoring compliance with the regulated entity's conflict of interest policy and oversight of investigations of conflicts of interest and unethical conduct.

13) Ensuring that the regulated entity has an adequate and effective system of internal controls that is implemented and maintained by competent and appropriately trained personnel by:

    a) Reviewing the regulated entity's internal control system and the resolution of identified material weaknesses and reportable conditions in the internal control system, including the prevention or detection of management override or compromise of the internal control system; and
    b) Reviewing the regulated entities programs and policies designed to provide reasonable assurance of compliance with applicable laws, regulations, and policies and monitoring the results of the compliance efforts.

14) Periodic reporting of its findings to the regulated entity's board of directors.

15) Ensuring that the external auditor provides the required communications (see the American Institute of Certified Public Accountants' (AICPA) Statement on Auditing Standards No. 114, *The Auditor's Communication with Those Charged with Governance* and the Public Company Accounting Oversight Board (PCAOB) Auditing Standard 5 - *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements.)* in a timely manner to the audit committee.

16) Reviewing and approving the financial statements and related disclosures prior to issuance.

Internal Audit Charter

The purpose, authority, and responsibility of the internal audit function must also be formally defined in a written charter that is approved, and periodically reviewed and re-approved, by the board of directors. The internal audit charter establishes the internal audit function's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of audit engagements; and defines the scope of internal audit activities. The charter should establish independence, which is defined in the *Standards* as the freedom from conditions that threaten the ability of the internal audit function to carry out responsibilities in an unbiased manner. The charter should also stipulate that the audit function have the resources needed in order for it to complete its work effectively and in a timely manner.

Internal Audit Function

Each regulated entity should have an effective audit program that is appropriate to the organization's size, and the nature and scope of its activities. The audit program should be effective in identifying issues, and the identification should be timely. Internal audit should be a risk-based, continuous function, coupled with well-planned external audit activity.

The internal audit function generally reviews transactions and decisions after the fact, and therefore functions as a detective control to identify problems, weaknesses, or errors after they occur. This distinguishes the internal audit function from the regulated entity's enterprise risk management function, which should be designed to identify and manage potential risks across the entity's operations – a preventive control. While the *Standards* require the internal audit function to evaluate the effectiveness of the regulated entity's risk management processes, the two functions should be separate and not be comingled. To the extent that the internal audit function provides assurance that the regulated entity's internal controls are effective, it can also be considered a preventive control. Additionally, an effective internal audit function may dissuade individuals from unauthorized and/or unallowable activities, which serves as a preventive control.

An effective internal audit function should exhibit the following characteristics:

1) Organizational Status

   Proper organizational status is necessary to ensure the independence and objectivity of internal audit. Without the support of the board of directors and senior management, the internal auditors may not receive the cooperation necessary to perform their tasks.

   If individuals move to internal audit from other divisions within the entity, they must refrain from assessing specific operations for which they were previously responsible; however, they may provide consulting services to the business staff relating to operations for which they had previous responsibilities. Objectivity is presumed to be impaired if an auditor provides assurance services for an activity for which the auditor had responsibility within the previous year. Internal auditors should not accept responsibility for non-audit functions that are subject to periodic internal audit assessments. If an internal auditor accepts responsibility for functions that are part of the internal audit plan a third-party entity or external auditors should complete audits of those areas. When internal audit staff works on a special project or consulting engagement they can offer recommendations, but should never participate in implementing those recommendations.

   If independence or objectivity is impaired in fact or in appearance, the details of the impairment should be disclosed to the audit committee of the board of directors. The nature of the disclosure will depend upon the impairment.

2) Professional Competency and Due Professional Care

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. Internal auditors must enhance their knowledge, skills, and other competencies through continuing education. Internal auditors should have knowledge of key information technology risk and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is a specific area, such as information technology auditing.

The internal audit director must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit function and continuously monitors its effectiveness. The process should include internal and external assessments. Internal assessments include ongoing reviews of the performance of the internal audit activity as well as periodic reviews through assessments by others within the organization that are knowledgeable of internal audit practices and the *Standards*. The *Standards* require that external assessments, such as quality assurance reviews, be conducted at least once every five years by a qualified, independent reviewer from outside the regulated entity. The results of the external assessment should be reported to the audit committee and the board of directors.

3) Management of Internal Audit Activities

The audit director must develop an annual audit plan that outlines the priorities of internal audit, consistent with the regulated entity's goals. The annual audit plan should be based on internal audit's assessment of risk for the entity's significant business activities, and should include input from senior management and the board of directors in the process. The audit director should also consider risk assessments performed by the business lines and the risk management function. Internal audit's risk assessment should analyze the risks inherent in a given business line, the mitigating control processes, and the residual risk exposure to the entity. Upon approval of the annual audit plan by the audit committee, internal audit should develop programs that describe the audit objectives and list the procedures that will be performed during each internal audit review.

The frequency of the audits should be consistent with the nature, complexity, and risk of the entity's business and operational activities. Specific items that may be considered in determining audit frequency include, but are not limited to, prior period audit results; identified weaknesses; organizational environment and changes; changes in key personnel, management oversight; adequacy of internal controls, policies and procedures; significance to the balance sheet and income statements or even significant changes to material balance sheet or income statement accounts; transaction volume; adequacy of systems; regulatory requirements and changes;

manual or systemic processing changes; change in market/business environment; and the adequacy of business contingency plans.

Audit work schedules should be sufficiently flexible to cover unanticipated demands on the internal auditing department. The *Standards* require that internal audit staffing resources should be appropriate, sufficient, and effectively deployed to achieve the approved plan. The audit director should report the audit plan and resource requirements, including significant interim changes, to senior management and the audit committee for review and approval, highlighting any resource limitations.

4) Communication

a) Audit Reports

Each report should include the audit's objectives and scope as well as applicable conclusions, recommendations, action plans, and where appropriate, the internal auditor's opinions and conclusions. The audit director or designee is responsible to review and approve the final audit report before issuance and should decide to whom the report will be distributed. If the auditor identifies significant risk management, control, and governance issues, such issues should be communicated promptly to senior management and the board of directors. When noncompliance with the *Standards* affects a specific engagement, communication of the results should disclose the *Standard(s)* with which full compliance was not achieved, the reason(s) for noncompliance, and the effect of noncompliance on the engagement.

b) Monitoring Results and Follow-up

The audit director must establish a process to monitor and follow-up on the findings to determine whether corrective action has been effectively implemented or that senior management has acknowledged and accepted the risk of not taking action. In addition, the internal audit department should determine whether violations, findings, weaknesses, and other issues reported by regulators (including FHFA), external auditors, and others have been promptly addressed. If corrective action has not been implemented, or if the audit director believes that senior management has accepted excessive risk, the audit director should engage in discussion with senior management. If the implementation or risk issue is not resolved, the matter must be reported to the audit committee. The audit committee should address the issue and disclose as appropriate to the full board of directors.

External Audit Activities

The external audit program should determine whether an entity's financial statements have been properly prepared in accordance with generally accepted accounting principles

(GAAP) consistently applied and to alert management to any material weaknesses or significant deficiencies in internal controls over financial reporting. There are four common types of independent public accountant's opinions:

1) Unqualified: States that the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with GAAP consistently applied.
2) Qualified: States that, except for the effects of the matter(s) to which the qualification relates, the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with GAAP consistently applied.
3) Adverse: States that the financial statements do not present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with GAAP consistently applied.
4) Disclaimer of Opinion: States that the auditor does not express an opinion on the financial statements.

The major factor that should be considered in evaluating the work of external auditors is the adequacy of the audit program. Examiners are interested in the work performed by external auditors for three principal reasons. First, situations will arise where internal audit work is not being performed or where such work is deemed to be of limited value to the examiner. In such situations, the work performed by external auditors should be reviewed to determine if it may be relied upon in lieu of the examiners performing the necessary verification procedures to compensate for an inadequate internal audit. Second, the work performed by external auditors may affect the amount of testing the examiner must perform. Third, reports rendered by external auditors often provide the examiner with information pertinent to the development of the examination scope or the conduct of the examination.

The PCAOB, created by Sarbanes-Oxley, establishes auditing and related professional practice standards for registered public accounting firms to follow in the preparation and issuance of audit reports. PCAOB Rule 3100, *Compliance with Auditing and Related Professional Practice Standards*, requires the auditor to comply with all applicable auditing and related professional practice standards of the PCAOB. The PCAOB has also adopted, as interim standards, certain preexisting standards of the AICPA generally accepted auditing standards.

In contrast with GAAP, generally accepted auditing standards (GAAS) are concerned with the auditor's professional qualifications, the judgment the auditor exercises in the performance of an audit, and the quality of the audit reports. GAAS are grouped into three categories: 1) general standards; 2) standards of field work; and 3) standards of reporting.

1) *General Standards:*

   a) The audit is to be performed by a person or persons having adequate technical training and proficiency as an auditor.
   b) Independence in mental attitude is to be maintained in all matters relating to the audit.
   c) Due professional care is to be exercised in the performance of the audit and the preparation of the report.

2) *Field Work Standards:*

   a) The work is to be adequately planned and any assistants are to be properly supervised.
   b) A sufficient understanding of the internal control structure is to be obtained to plan the audit and to determine the nature, timing, and extent of tests to be performed.
   c) Sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmations to afford a reasonable basis for an opinion regarding the financial statements under examination.

3) *Standards of Reporting:*

   a) The report shall state whether the financial statements are presented in accordance with GAAP.
   b) The report shall state whether GAAP has been consistently applied in the current and preceding periods.
   c) Informative disclosures in the financial statements are to be reasonably adequate unless otherwise stated in the report.
   d) The report shall contain either an expression of opinion on the financial statements, taken as a whole, or an assertion that an opinion cannot be expressed.

Regulatory Environment

The primary authorities governing, or relevant to, external and internal audit activities of the regulated entities are set forth below. The examiner should review these to ensure compliance.

1) Rules and Regulations of the Federal Housing Finance Agency and its predecessor, the Federal Housing Finance Board (Finance Board), which include the following parts and sections relevant to the FHLBank's internal and external audit function:

12 CFR Part 917 of the Finance Board regulations addresses the powers, responsibilities, and accountability of FHLBank boards of directors and senior

management by prescribing standards for a corporate governance framework. In particular:

12 CFR 917.2, *General authorities and duties of Bank boards of directors*, includes a provision that each Bank director shall have the ability to understand a Bank's balance sheet and income statement and ask substantive questions of management and the internal and external auditors.

12 CFR 917.3, *Risk management*, requires that each Bank's board of directors have a risk management policy that addresses the Bank's exposure to credit risk, market risk, liquidity risk and operations risk.

12 CFR 917.6, *Internal control system*, requires that each Bank shall establish and maintain an effective internal control system which, for example, directs senior management to address concerns expressed by internal auditors, external auditors and regulatory examiners regarding weaknesses in the internal control system.

12 CFR 917.7, *Audit committees*, addresses the powers, duties, composition, and responsibilities of the audit committees. These responsibilities should be detailed in a charter and approved by the board of directors. The duties of each Bank's audit committee include overseeing the internal audit and external audit functions and in that connection reviewing and approving the internal auditor's work plan and approving the external auditor's annual engagement letter. The audit committee also has the duty to assess the performance of the internal auditor and external auditor.

12 CFR Part 1273 of FHFA regulations sets forth the requirements for the Office of Finance and the combined financial reports, Board and Audit Committee requirements. In particular:

12 CFR 1273.3 (b) addresses the preparation of combined financial statements.

12 CFR 1273.4 (c) states that FHFA shall determine whether a combined Federal Home Loan Bank System annual or quarterly financial report complies with the standards of part 1273.

12 CFR 1273.6 (b) states the requirements of combined financial reports.

12 CFR 1273.8 (a) (3) requires that each director of the Office of Finance board of directors have the ability to ask substantive questions of management and the internal and external auditors about the combined financial statements of the Federal Home Loan Bank System and the operations and financial statements of the OF.

12 CFR 1273.9 addresses the responsibilities of the OF Audit Committee, including overseeing the internal audit activities, employing the services of an independent, external auditor, reviewing the external auditor's opinion on the financial statements, ensuring that senior management is maintaining an adequate internal control system within the OF, and providing an independent direct channel of communication between the OF's board and the internal and external auditors.

12 CFR Part 1274 of FHFA regulations sets forth standards related to the financial statements and related external audits of the FHLBanks, the Office of Finance, and the Financing Corporation.

12 CFR 1274.1 defines an audit and an audit report.

12 CFR 1274.2 (a) requires each Bank, the OF and the Finance Corporation of the Federal Home Loan Bank System (FICO) to obtain annually an independent audit and audit report on its financial statement.

12 CFR 1274.2 (b) requires the OF audit committee to obtain an audit and audit report on the combined annual financial statements for the Bank System.

12 CFR 1274.2 (c) requires that all audits must be conducted in accordance with generally accepted auditing standards and in accordance with the current government auditing standards of the Office of the Comptroller General of the United States (i.e., the U.S. Government Accountability Office).

12 CFR 1274.2 (d) requires that an independent, external auditor must meet at least twice a year with the audit committee of each Bank, the audit committee of the OF, and the related Financing Corporation (FICO) Directorate.

12 CFR 1274.2 (e) requires that examiners shall have unrestricted access to all auditors' workpapers and to the auditors to address substantive accounting issues that may arise during the course of any audit.

12 CFR 1274.3 addresses requirements to provide financial and other information to FHFA and the OF.

2) Rules, Regulations, and Orders of the Federal Housing Finance Agency and its predecessor, the Office of Federal Housing Enterprise Oversight (OFHEO), which include the following parts and sections relevant to the Enterprises' internal and external audit function:

12 CFR Part 1710 of the OFHEO regulations addresses powers and responsibilities of the boards of directors for Fannie Mae and Freddie Mac. In particular, 12 CFR

1710.12 requires the establishment of an audit committee.

FHFA Order No. 2008-006 states that the members of the board and board committees shall function in accordance with the applicable designated duties and with the authorities as set forth in federal statutes, regulations, and FHFA examination and policy guidance, Delaware law (for Fannie Mae), Virginia law (for Freddie Mac) pursuant to FHFA regulation 12 CFR 1710.10, and in the bylaws and applicable committee charters in existence as of the date of the order. The bylaws and committee charters may be amended or modified by, or with the consent of, FHFA as conservator.

3) Rules and Regulations of the Federal Housing Finance Agency, which include the following parts and sections relevant to the internal and external audit function:

12 CFR part 1236 Prudential Management and Operations Standards (PMOS) Standard 2 (Independence and Adequacy of Internal Audit Systems) highlights the need for an independent audit function, the need for the regulated entity to establish an internal audit function that adequately tests internal controls, the audit committee responsibilities related to the internal audit function, and ensuring the audit function conducts risk-based audits and the audit function is properly staffed.

4) Advisory Bulletins and Resolutions of the Federal Housing Finance Agency, and its predecessor, the Finance Board that provide guidance related to internal/external audit include the following:

Advisory Bulletin 2013-03 (FHFA Examination Rating System) dated December 19, 2012, contains guidance and evaluative factors pertaining to internal audit under the "Management" component rating. The evaluative factors include conformance with internal policies and controls, adequacy of audits, and responsiveness to findings made by internal and external audit functions or outside consultants.

Advisory Bulletin 96-1, (Internal Audit Independence) dated February 29, 1996, provides that the Audit Committee is responsible for the selection, compensation and performance evaluation of the CAE

Advisory Bulletin 02-5, (Risk Assessment – Internal Audit Independence) dated April 8, 2002, provides that the internal audit function should not take an ownership role and manage or coordinate the annual risk assessment of the FHLBank.

Advisory Bulletin 05-05, (Risk Management Oversight) dated May 18, 2005, provides guidance on the risk management responsibilities of the Board, senior management, and risk management.

Federal Housing Finance Board Resolution numbered 92-568.1, dated July 22, 1992, sets forth minimum standards for the internal audit function and CAE.

5) Other Supervisory and Examination Guidance issued by the FHFA

FHFA Examination Guidance: Examination for Accounting Practices dated October 27, 2009, sets forth guidance relevant to Audit Committees, internal audit functions, financial statements, and external audit functions.

6) Regulations and interpretations of the Securities and Exchange Commission. The below SEC rules and regulations are designed to ensure the organization discloses meaningful financial information to the public and enforces the securities laws.

Securities Exchange Act of 1934, Section 10A (g) Prohibited Activities.
SEC Rule 10A-3 Standards Relating to Listed Company Audit Committees.
SEC Rule, Revision of the Commission's Auditor Independence Requirements.
SEC Regulation S-X [17 CFR Part 210], Rule 2-01, Qualifications and Reports of Accountants.
SEC Regulation S-K [17 CFR Part 229], Section 229.303 (Item 303), Management's Discussion and Analysis of Financial Condition and Results of Operations.

In addition, SEC Regulation S-K [17 CFR Part 229], Section 229.306 (Item 306), sets forth requirements pertaining to audit committees and SEC Regulation S-K [17 CFR Part 229], Section 229.407 (Item 407), Corporate Governance addresses various corporate governance requirements that relate to the Board and audit committee.

7) The Public Company Accounting Oversight Board Rule 3100, Compliance with Auditing and Related Professional Practice Standards, requires external auditor to comply with all applicable auditing and related professional practices standards of the PCAOB.

8) Sarbanes-Oxley Act of 2002 **(Sarbanes-Oxley),** addresses various corporate governance requirements that relate to the Board, internal and external audit functions, and management's attestation surrounding ICFR. In particular, section 301 sets forth standards related to audit committees.

9) New York Stock Exchange Rule 303A, sets forth corporate governance rules with specific standards for Audit Committees.

10) Professional standards adopted by the Institute of Internal Auditors. The Institute of Internal Auditors (IIA) provides authoritative certification, education, research, and technological guidance for the profession. The IIA serves as the profession's resource on significant auditing issues worldwide and issues the Standards for the Professional Practice of Internal Auditing and the International Professional Practices Framework.

11) ***Financial Accounting Standards Board (FASB) Codification.*** FASB is the single source of authoritative U.S. generally accepted accounting principles governing the preparation of financial reports and is officially recognized as authoritative by the SEC and the AICPA. Effective July 1, 2009, changes to the source of authoritative U.S. GAAP, the *FASB Accounting Standards Codification*, are communicated through an Accounting Standards Update (Update or ASU). Updates are published for all authoritative U.S. GAAP promulgated by the FASB, regardless of the form in which such guidance may have been issued prior to release of the FASB codification (e.g., FASB Statements, EITF Abstracts, FASB Staff Positions). Updates also will be issued for amendments to the SEC content in the FASB codification as well as for editorial changes.

An Update is a transmittal document that (1) summarizes the key provisions of the project that led to the Update, (2) details the specific amendments to the FASB codification, and (3) explains the basis for the Board's decisions. Although ASUs update the FASB codification, the FASB does not consider Updates as authoritative in their own right.

Prior to the release of the FASB codification as the single source of authoritative U.S. GAAP, the FASB amended pre-codification standards and issued them in an "as amended" form. Now, the FASB will not amend Updates. It will only amend the FASB Codification.

Issues Specific to the Regulated Entities

Audit cycles may vary amongst the regulated entities; however, they should always be commensurate with the assigned risk rating. Typically, audits rated high risk will be conducted annually, medium risk audits may be conducted once every two years, and low risk audits may be performed on a three-year cycle. If a regulated entity's audit cycles allow greater latitude than this, the basis should be documented, justified, and approved by the audit committee.

The external and internal auditors should coordinate the timing and scope of their audits within a regulated entity to ensure adequate coverage of the major risks and to minimize duplication of effort. With respect to the FHLBanks and the Office of Finance, one public accounting firm is responsible for performing the financial statement audits of the separate entities, as well as the combined financial statements for the FHLBank System. The regulated entities may engage different public accounting firms to perform the external audit programs; however, the external auditor selected by the regulated entity must adhere to the standards in FHFA's *External Auditor Review* guidance and the PCAOB's *Appointment of the Independent Auditor*.

The specific number of internal auditors, reporting structure of the audit function, background, experience, education, and professional certifications of the audit staff, audit methodologies, and practices may vary among regulated entities due to unique factors, such as business strategies, and internal competencies. Specific engagements may be outsourced or co-sourced for various reasons ranging from insufficient staff to complete planned audits timely, to a need to obtain technical expertise for a particular audit that is beyond that needed to conduct most audits of an entity's operations.

If an internal audit engagement is outsourced, examiners should consider reviewing the objectives detailed in the engagement letter, scope of review, audit committee approval, coordination with internal auditors and senior management, testing, reporting the results to senior management, corrective action, and reporting to the audit committee and the board of directors. Examiners should also consider the number and type of outsourced audits when assessing the adequacy of resources and expertise of the internal audit function.

When evaluating the adequacy of the internal audit function, examiners should consider reviewing the internal auditor's procedures against actual practices, the timely completion of audits, and the adequacy of internal audit resources. The examiners should be alert to potential weaknesses or deficiencies that relate to audit independence, risk assessment, development of the audit universe and annual plan, audit programs, testing methodologies, workpaper documentation, evaluation of findings, supervision of the work performed, audit reports, and communications to management and the board of directors.

Examination Guidance

The workprogram for the Internal and External Audit 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 analysis, 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 institution's audit 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

Evaluate the independence, scope of responsibility, and objectivity of the internal audit function and independence of the external auditor. Specific worksteps include, but are not limited to, the following:

1) Review past reports of examination for outstanding issues or previous problems related to internal audit and/or external audit.

2) Review FHFA off-site monitoring or analysis reports, and workpapers produced as part of on-going monitoring, related to internal audit and/or external audit.

3) Assess the status of outstanding examination findings pertaining to internal audit and/or external audit.

4) Review minutes of meetings of the board of directors, audit committee and other relevant board and management committees for any issues regarding internal audit and/or external audit.

5) Determine if the purpose, authority, and responsibility of internal audit has been formally defined in a charter that has been approved by the audit committee.

6) Determine if the charter establishes the internal audit department's position within the regulated entity, authorizes unrestricted access to records, personnel, and physical properties relevant to the performance of audits, defines the scope of internal audit activities, addresses consulting activities, and is periodically reviewed by the audit committee.

7) Determine if the internal audit function has a code of ethics that adequately addresses the principles and rules of conduct that are relevant to the profession and practice of internal auditing.

8) Contact the FHFA's Office of the Chief Accountant to obtain and evaluate any applicable information from their external auditor workpaper review regarding the assessment of the internal audit function.

9) Review the external auditor's opinion on internal audit reliance that was reported to the audit committee. *(Does the opinion cast any doubts on the reliability of the internal audit department's work?)*

Summarize the work performed in the examination of the internal and external audit 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.

2. Description of Risks

Evaluate the internal audit director's methodology for managing the audit department and whether internal audit contributes materially to the improvement of the organization's risk management, control and governance. Evaluate the audit committee's engagement of the external auditor and communications with the external auditor, and whether they conform with FHFA regulations and guidance. Specific worksteps to consider include the following:

1) Determine if the internal audit department policies and procedures comply with the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*. *(Do policies and procedures provide sufficient guidance to understand and comply with the Standards?)*

2) Review and assess the internal auditor's annual risk assessment plan and results and how it connects to the audit universe and annual audit plan. *(Does the audit universe and audit plan appropriately address and budget for high risk areas?)*

3) Review and evaluate the audit universe and annual audit plan to determine if they are based on internal audit's assessment of risk, include input of senior management and the board of directors and audit committee, and consider consulting assignments.

4) Determine if internal audit resources are appropriate, sufficient and effectively deployed to achieve the audit plan. *(Is the audit plan completed on schedule without the need to postpone audits to the next cycle?)*

5) Review the annual audit plan to determine if it covers significant risks of the regulated entity and the frequency of those audits.

6) Review and evaluate departmental policies and procedures to determine if they provide an adequate guide to the audit staff. *(Do the policies and procedures simply mirror the IIA Standards or do they provide sufficient guidance on how to comply with the IIA Standards?)*

7) Determine if the internal audit department participates on any management committees, as well as, the development of new systems and products, and if so assess internal audit's role(s). *(Is internal audit a voting member on a committee responsible for taking on risk, which would jeopardize independence?)*

8) Determine if the internal audit function is adequately coordinated with the external auditors and outside consultants to ensure proper coverage and minimize duplication of efforts.

9) Review and evaluate periodic reports provided to the board of directors and senior management on the internal audit performance relative to the annual audit plan, that report significant risk exposures and control issues, corporate governance issues, and other matters needed or requested by the board of directors and senior management.

10) Review any internal assessments, including ongoing reviews of the performance of the internal audit or consulting engagement such as the supervision of the engagement, review of workpapers and the final report, and surveys with senior management ensuring that audit workpapers support the conclusions drawn in the report. *(Are issues reported to the appropriate individuals within the organization?)*

11) Review any external assessments, such as quality assurance reviews which are required by the *Standards* to be performed every five years. *(Have recommendations included in the external assessments been implemented by internal audit?)*

3. Risk Management

Assess the regulated entity's adequacy of audit function internal controls and efforts to remediate identified weaknesses. Specific worksteps to consider include:

Risk Identification Process

1) Assess the adequacy of the internal auditors' 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. As part of the assessment, evaluate preplanning, fieldwork, supervision, reporting, follow-up, and consulting services.

2) Evaluate the effectiveness of external auditor's engagement letters, formal reports, and management letters that have been communicated to senior management in identifying and addressing significant risks to the regulated entity. *(Are the engagement letters "boilerplate" or are they tailored to the regulated entity's risk profile? Do the reports provide sufficient detail on areas that need corrective action?)*

3) Assess the external auditor's communications to the audit committee for their effectiveness in focusing the audit program on areas of high risk and the extent and effectiveness of coordination between external and internal audit activities. Refer to Sarbanes-Oxley Section 204. Specific areas to consider include:

    a) Indemnification clauses which limit or release the external auditor from liability for negligent acts are excluded from the engagement letter.
    b) Annual report that discloses the external auditor's opinion on the presentation of the financial statements, and, when applicable, the external auditor's report on management's assertions over financial reporting.
    c) Management letters that address other matters or issues to senior management.
    d) Report to the audit committee which includes, but is not limited to, the following:

        i. Responsibility of the independent external auditors, and communications to the audit committee.
        ii. Scope and results of the annual audit, internal audit reliance and management cooperation.
        iii. Report on compliance with certain laws and regulations and on internal controls over financial reporting as well as significant accounting, auditing and reporting matters.
        iv. Emerging accounting and reporting issues, regulatory matters, and other

services rendered.
v. Independence.

4) Evaluate the adequacy of the objectives and scopes of any outsourced reviews and determine the status of management's actions regarding recommendations. *(How has internal audit responded to the consultant recommendations?)*

5) Assess the communications to the audit committee that address the following subjects:

   a) Significant accounting policies, including the external auditor's judgment of the quality of the accounting policies and the consistency of the application of those policies and alternative accounting treatments with GAAP.
   b) Management judgments and accounting estimates, audit adjustments, and potential effects on the financial statements of any significant risks and exposures.
   c) Fraud and other illegal acts and deficiencies in internal control.
   d) Material uncertainties related to events and conditions, including going concern issues.
   e) Other information in documents containing audited financial information.
   f) Disagreements with management and difficulties encountered in performing the audit.
   g) Consultations with other accountants.
   h) Major issues discussed with management prior to retention.
   i) Responsibilities of the audit committee.
   j) FHFA examination findings and management's progress in remediating those findings.

Organizational Structure

1) Review the organization chart to determine internal audit independence and determine if the internal auditor reports directly to the audit committee on substantive matters and is ultimately accountable to the audit committee and the board of directors. *(Does the internal audit director report directly to the CEO on issues other than administrative matters?)*

2) Review staff resumes to determine if education, experience, training and professional certifications of the audit staff appear sufficient to perform their duties and responsibilities. *(Does the audit staff have specialized expertise on highly technical functions performed by the regulated entity?)*

3) Evaluate the qualifications and independence of audit committee members. For FHLBanks, determine if at least one member of the audit committee has extensive accounting or financial management experience as required by 12 CFR 917.7.

4) Review and evaluate the audit committee charter. Determine if the formal definition

of the purpose, authority and responsibility of the audit committee was approved by the board of directors. With respect to FHLBanks, determine compliance with 12 CFR 917.7, which requires re-approval of the audit committee charter at least every three years.

5) Review and assess the compensation and performance evaluation of the internal audit director. *(Is this evaluation performed by the audit committee? Is the independence of the internal audit function compromised by the influence of the CEO? Do the internal audit director's compensation standards ensure there will not be a conflict of interest in carrying-out job responsibilities in an objective fashion?)*

Reporting

1) Review and evaluate the adequacy of information reported to the audit committee which includes, but is not limited to, the following:

   a) Minutes of prior meetings that have been presented to and approved by the audit committee.
   b) Status of the current audit plan and other audit matters, such as performance, personnel, training and budgets.
   c) Prior audit and consulting reports and management's responses.
   d) Summaries of significant risk exposures and control issues, corporate governance issues and other matters needed or requested by the board of directors or senior management, such as new regulatory or accounting requirements, employee related issues and contingent litigation.
   e) Tracking and reporting the status of previously reported findings.
   f) External auditors' and third-party reports, presentations and SSAE 16 reviews on key/critical service providers.

2) Review and evaluate periodic reporting by the audit committee chairman to the board of directors. *(Are the reports comprehensive or do they simply state the status of the annual audit plan schedule?)*

Information Technology

1) Interview internal audit staff to determine if they have knowledge of key information technology (IT) risks and controls and available technology-based audit techniques necessary to perform their assigned work, understanding they may not have the expertise of an IT auditor and contract that work out. *(Does the internal audit staff have sufficient knowledge and expertise to review the work of an IT contractor or outsourced audit?)*

Compliance

1) Review and evaluate the implementation and administration of whistleblower policies and procedures complying with Sarbanes-Oxley requirements.
   a) Verify the audit committee has established procedures for the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, or auditing matters, including procedures for employees to confidentially and anonymously submit concerns on accounting or auditing matters. (Sarbanes-Oxley Section 301.)
   b) Verify any investigation into a submission does not in any way discriminate against the employee who disclosed their concerns. (Sarbanes-Oxley Section 806.)

2) Assess compliance with FHFA PMOS Standard 2 (Independence and Adequacy of Internal Audit System). Specifically:

   a) Verify that the regulated entity's board of directors has established an audit committee whose responsibilities include ensuring the independence of the internal audit function and that the internal audit staff is trained and competent.
   b) Verify that the board of directors reviews and approves the audit committee charter at least every three years.
   c) Determine that the audit committee evaluates the effectiveness of the internal audit function.
   d) Evaluate the promptness and adequacy of responses provided to the audit committee concerning internal audit reports.
   e) Evaluate and assess internal audit's effectiveness in monitoring the adequacy of the regulated entity's internal controls.
   f) Evaluate the independence of internal audit.
   g) Evaluate the staffing resources (competency and resource numbers) of the internal audit staff.
   h) Determine if internal audit conducts risk-based audits based on a risk-based organizational assessment.
   i) Verify that internal audit conducts adequate testing and review of internal control and information systems.
   j) Verify that internal audit takes adequate steps to ensure that any violations, findings, weaknesses, and other issues reported by regulators, external auditors, and others are promptly addressed and satisfactorily resolved.

3) Determine compliance with FHFA's *External Auditor Review* guidance and the PCAOB's *Appointment of the Independent Auditor*.

4. Testing

Given the nature of examination work, specifically, the fact that it is usually impractical to test 100 percent of workpapers, examiners typically use risk-based, judgmental, nonstatistical sampling whereby they rely on their professional experience and knowledge to determine the appropriate sample. When choosing a sample, examiners should consider a number of factors in order to optimize the representative quality of the sample. Those factors should include the nature of the risk of the audited activity as reflected in the department's risk assessment. High risk activities may warrant a larger sample than lower risk activities. Examiners should select samples from the audit work performed under the supervision of the various audit managers given that the quality of individual audit engagements may differ across audit managers. When examiners are projecting the results of judgmental sampling to the entire population of internal audit work, examiners should ensure that they have sampled an appropriate number of audits relative to the entire audit population to reduce sample error. For further guidance on the review of specific internal audits, see Appendix A at the end of this module.

1) Select a sample of recently completed internal audits and evaluate the adequacy of the scope, testing, and workpapers completed by internal audit and determine the status of corrective actions for findings.

2) Review and evaluate training to address the continuing professional development of the audit staff.

3) Select a sample of recently completed audits that were outsourced and evaluate the adequacy of the scope, testing, and workpapers completed by internal audit and determine the status of corrective actions for findings. Specifically:

    a) Obtain and review the following documents:

        i. Outsourced internal audit arrangement contracts or engagement letters.
        ii. Outsourced internal audit reports.
        iii. Outsourced audit policies, if any.

    b) Review the outsourcing arrangement contract/engagement letter between the contractor and regulated entity and determine whether the contract/letter adequately:

        i. Defines the expectations and responsibilities under the contract for both parties.

ii. Sets the scope, frequency, and fees to be paid for work to be performed by the outside contractor.
iii. Describes responsibilities for providing and receiving information, such as the type and frequency of contractor reporting to the regulated entity's audit manager, senior management, and audit committee or board of directors about the results and status of work.
iv. Establishes protocol for changing the terms of the engagement, especially for expansion of audit work if significant issues arise, as well as stipulations for default and termination of the contract.
v. States that internal audit reports are the property of the regulated entity and specifies ownership of internal audit workpapers. If the contractor retains ownership of the workpapers, the contract should stipulate that the regulated entity will be provided copies of related workpapers that the entity deems necessary, and that regulated entity employees will have reasonable and timely access to contractor workpapers.
vi. Notes that the contractor's audit activities are subject to FHFA review and that examiners will be granted full and timely access to all related outsourced internal audit reports, audit programs, audit workpapers, and memorandums and correspondence prepared by the outsourced contractor.
vii. Specifies the location and for how long the contractor will retain outsourced internal audit reports and related workpapers. If the workpapers are in electronic format, the agreement should address contractor maintenance of proprietary software to facilitate access and review by the regulated entity or the examiners.
viii. Establishes processes for determining who bears the cost of consequential damages arising from errors, omissions, and negligence.
ix. States that the contractor will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to a member of regulated entity management or regulated entity employee. As applicable, states the contractor will comply with professional and regulatory independence guidance.

c) Determine, through discussions with regulated entity management or review of applicable documentation, whether the board of directors or audit committee performed sufficient due diligence to satisfy themselves of the contractor's competence and objectivity prior to entering the outsourcing arrangement. Consider whether due diligence addressed the following:

i. Available contractor services (including specialized areas) and work arrangements.
ii. Costs and benefits of contractor services to be provided.
iii. Ability and flexibility of contractor to perform the services in a timely manner and maintain the confidentiality of regulated entity data.

iv. Experience level, technical expertise, and credentials of contractor staff (including specialized areas such as information technology, international, trust, and capital markets).
v. Notifications of any changes in contractor processes, staffing, or other changes affecting assigned staff.
vi. Contractor's approach for conducting outsourced internal audits (e.g., risk-based or traditional, use of audit tools and audit technology).
vii. Reference checks.
viii. Contractor's internal quality control processes (peer review and quality assurance).
ix. Discussions of contractor independence, objectivity, integrity, and conflict of interest standards, e.g., AICPA, IIA, PCAOB, and SEC.

d) Arrange a meeting with the contractor and discuss the outsourced internal audit program. Consider:

i. Contractor's understanding of the regulated entity's risk profile and business.
ii. Contractor's sampling techniques for testing internal controls.
iii. Contractor's training program for its audit staff.
iv. Communication with and reporting to the regulated entity's board of directors, audit committee, and management.
v. Whether the contractor's audit procedures are customized for each regulated entity client or are generic.
vi. Contractor's method for reviewing internal controls.
vii. Methods used to structure contracts.
viii. How the contractor ensures independence/coordination with external audit activities.
ix. Workpaper documentation standards.

e) Determine how the regulated entity and contractor address control weaknesses or other matters noted by the outsourced contractor. Consider whether:

i. The contractor reports results of outsourced internal audit work to the regulated entity's audit manager or internal auditor in a timely manner.
ii. The contractor has access to the board of directors or the audit committee to independently report findings when necessary. *(If not, how are findings communicated? Are concerns communicated to both the board and senior management appropriately?)*

f) Review outsourced internal audit reports issued and a sample of outsourced internal audit workpapers to determine their adequacy and preparation in accordance with the audit program and the outsourcing agreement for the regulated entity. Determine whether:

i. Workprogram steps, calculations, or other evidence support the audit scope's objectives, procedures and conclusions set forth in the outsourced internal audit reports.
ii. The scope of the outsourced internal audit procedures and work is adequate in light of risk and control assessments for the area audited.
iii. The workprogram and audit reports adequately document material findings, including root causes of significant weaknesses, and whether follow-up on noted weaknesses and promised corrective action is adequate.

g) Determine whether the scope of outsourced audit work is revised appropriately when the regulated entity's environment, activities, risk exposures, or systems change.

For additional guidance, the FHFA's Office of the Chief Accountant has provided suggested procedures and comments for completing the review of the regulated entities' internal audit. See attachment at the end of this module entitled "Guidance for the Review of Specific Internal Audits."

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 internal audit and/or external audit function. Develop a memorandum articulating the risks to the institution related to internal audit and/or external audit and 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 regulated entity is exposed 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 regulated entity'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 institution and the potential effect to the regulated entity 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 to remediate the finding. Communicate preliminary findings to the EIC. Discuss findings with regulated entity personnel to ensure the findings are free of factual errors or misrepresentations in the analysis.

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 raise to the level of a finding. Potential concerns include issues the regulated entity is in the process of addressing, but require follow-up work to ensure actions are completed appropriately. In addition, potential concerns should include anticipated changes to the institution's practices or anticipated external changes that could affect the institution's internal audit and/or external audit function.

Workprogram

1. Scope of Examination Work Performed

Workpapers must document the examination activities undertaken to evaluate potential risks related to internal audit and/or external audit.

2. Description of Risks

- Identify areas of concern related to internal audit and/or external audit
- Assess current risks and trends in the risk to the organization emanating from the internal audit and/or external audit 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 organization's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
    - The regulated entity's organizational structure
    - Policy and procedure development for internal audit and/or external audit
    - Appropriateness of risk metrics established for internal audit and/or external audit
    - Reporting by management and the board
- Assess and conclude on the adequacy of information technology and controls related to internal audit and/or external audit
- Assess and conclude on the adequacy of the organization'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 examination standards

5. Conclusions

- Summarize conclusions for all examination work performed related to internal audit and/or external audit
    - Conclude on the level of risk to the organization
    - Include an assessment of the adequacy of an organization'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

Appendix A

Guidance for the Review of Specific Internal Audits

The following provides suggested guidance for reviewing internal audits when completing workprograms in specific risk areas as part of the safety and soundness examination activities for a regulated entity. When evaluating testing of controls performed by the internal auditors for the area being reviewed, examiners should consider the following types of questions/procedures and related rationale, as applicable, when completing their analysis.

1. **Does the purpose and objective of internal audit's work tie-in with the internal audit department's annual Internal Audit plan?**

   Obtain a copy of the internal audit department's annual plan. If the work does not tie-in, you should consider why not.

2. **Are the risks related to the audit properly identified?**

   As part of the planning phase of an audit, the internal audit team will determine what risks are related to the area/process under audit. In certain areas, the key risks may be apparent given the industry and specific area. For example, loan loss reserves. However, identifying the key risk areas also involves other points such as internal audit brainstorming with the external audit team and management as it relates to the area under examination, reviewing prior year audit results, reviewing the external audit's risk assessment, factoring in department turnover or any reorganizations, etc.

   As an example, when planning an audit, the audit team should determine if there are other considerations that may expand the testing to be performed. For instance, if in the prior year audit of accounts payable, it was determined that invoices were often not properly authorized and payments were not properly coded for general ledger entry, which resulted in misstatement in the financial statements, these matters would be given higher weighting in the scope of this year's audit.

3. **Is the scope of the audit adequate to achieve the overall objective?**

   The scope of the audit should be based on what the internal audit team has determined are the key risks associated with this area. Continuing with the accounts payable audit example, has the internal audit team established an overall objective to obtain assurance that the internal controls surrounding the accounts payable function are effective, i.e., payments are properly authorized and coded

correctly. Another example would relate to the budgeted hours. If the audit work relates to a high risk area, does internal audit's budget include sufficient hours?

4. **Is the audit planned in accordance with the Internal Audit Department's Policies and Procedures?**

   The examiner would review the internal audit workpapers to determine if they were completed in accordance with the Internal Audit Department's policies and procedures. If the policies and procedures require for a budget to be prepared and for certain work be completed in advance prior to actual field work, was a budget prepared and was the pre-field work completed before commencement of the audit?

5. **Do internal audit personnel assigned to the audit in their respective capacity (staff, senior, manager, etc.) have appropriate credentials for their assigned role? Is there evidence of appropriate levels of review being conducted throughout the audit?**

   Internal Audits should be staffed with personnel that have the appropriate credentials for the role they are performing in the audit. For example, a high risk area audit of loan loss reserves should be staffed with experienced personnel. It would be reasonable to expect that team members on this audit have appropriate certifications, and some background/history with loan loss reserves. The examiner should also determine if appropriate levels of review are occurring. Was the staff auditor's work reviewed and signed-off by the senior auditor and manager?

6. **Do the audit tests appear to be reasonably designed to meet the audit objectives?**

   For example, if the audit objective is to determine whether internal controls surrounding accounts payable are effective, and one of the key risks identified is unauthorized payments, then it would be reasonable to expect that internal audit reviews payments made to ensure the required authorizations exist. This same rationale should follow each audit objective and risk identified during the planning process.

7. **Is the sampling methodology properly documented and supported?**

   In most instances it would not be feasible for internal audit to test 100 percent of the population under audit. As a consequence, internal audit uses various sampling methods when determining those items to test. It is a requirement that when sampling, the methodology be documented and the items selected for testing are identifiable by a person coming behind internal audit.

The examiner is not expected to opine on the sampling methodology utilized, just that it is documented. For example, the accounts payable group issued 300,000 checks. The audit team has opted to select 2,000 checks using a random number generator. The workpapers should document this information: 2,000 checks were selected using a random number generator. The check numbers identified by the random number generator need to be listed in the workpapers so that an examiner or other third party can verify those generated as part of the random sampling were included in the related testing.

8. **Do the results of the audit tests properly support the conclusions reached in the reports? Is the audit report clear and concise in its reporting of purpose, objectives, results and conclusions?**

   For example, if internal audit's testing noted exceptions but they were deemed not of significance for inclusion in internal audit's report, does this make sense? If they conclude the exception is isolated, does that appear to be reasonable?

9. **Are the results/recommendations communicated to management? Are management's responses to findings/recommendations reasonable and appropriate? Has internal audit followed up, or plan to follow up, on findings?**

   For example, if internal audit's testing noted numerous exceptions but their report concluded the controls were satisfactory, how does that reconcile with all the exceptions.

10. **The examiner should consider any other items or concerns noted during the examination that appear to be unresolved.**

    The key is that internal audit's work supports the conclusions reached and that there are no open or unresolved items that have not been properly flagged.