EM-31.3

Category: Board & Management Operations
Topic: Audit & Review Programs
Published: 1/7/2021

Overview

The *Audit & Review Programs* topic provides guidance on evaluating the oversight, staffing, activities, and effectiveness of a Farm Credit System (System) institution's audit and review programs. Institution boards and management are responsible for ensuring internal control systems exist and operate effectively. An important component of an effective internal control system is strong audit and review programs. Institutions incorporate preventive and detective internal controls into plans, policies, and procedures of each major operating function. Audit and review programs should detect weaknesses or errors and add value by identifying performance improvement opportunities. Personnel completing the work need to be independent of the function being audited or reviewed. The audit and review programs should assess the function's processes, controls, transactions, and decisions through review and testing. When properly structured and conducted, audit and review programs can provide the board, management, and third parties information about internal control system effectiveness. This enables management to take prompt action that will help achieve business objectives, strengthen internal controls, and prevent weaknesses. Audit and review programs are also a critical defense against fraud by validating internal controls are functioning effectively and by detecting potential fraudulent activity.

The board (or Audit Committee, if so delegated) is accountable for establishing, overseeing, and maintaining effective audit and review programs that:

- Identify an appropriate audit universe.
- Evaluate and test the adequacy of internal controls and efficiency of operations.
- Evaluate whether policies and procedures are sufficient and followed.
- Validate the reliability of financial statements and reporting.
- Confirm compliance with laws and regulations.
- Identify vulnerabilities to fraud and confirm adequate processes and controls are in place to reduce susceptibility to fraud.

The structure of an institution's audit and review programs depends on factors such as institution complexity, scope of activities, and business risk profile. While the board cannot delegate its accountability over audit and review programs, it may delegate responsibilities to an appropriate staff member.

Institutions should address how audit and review activities will be conducted in accordance with professional standards. The most common professional standards are within the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF). We use the International Standards for the Professional Practice of Internal Auditing from the IPPF as sound business practice criteria when examining an institution's audit and review programs. We refer to several specific

standards in the guidance below. There are also other professional standards that have applicability to internal audit and review programs, such as the American Institute of Certified Public Accountants (AICPA) Standards and Statements.

Professional standards address items such as independence, professional proficiency, scope of work, performance of work, internal audit management, quality control, and quality assurance reviews. Using professional standards will help audit and review programs address the risks and meet the demands posed by the institution's current and planned business activities. Examiners should take advantage of independent quality assurance reviews or other quality control assessments and consider these when evaluating effectiveness and reliability of audits and reviews. However, examiners should validate the auditor or reviewer competencies and quality of work performed before relying on the results from these reviews or assessments.

While this section focuses on internal audit and review programs, it also includes some guidance related to the external audit. References in this section to the external audit or external auditors are specifically referring to the financial statement audit performed by a qualified public accountant as required by Farm Credit Administration (FCA) Regulation 621.4.

Examination Procedures and Guidance

General

1. Audit Committee:

Evaluate the structure, operations, and effectiveness of the Audit Committee in overseeing audit and review programs and internal controls.

Guidance:

Institutions must establish an Audit Committee to assist the board in carrying out specific fiduciary duties. FCA Regulation 620.30 requires the committee to oversee financial reporting and related controls. However, the board may also delegate other roles to the committee. For example, this may include oversight of internal audit and review programs, oversight of the whistleblower program, and involvement in enterprise risk management processes. Examiners should review documents such as the committee charter, meeting minutes, policies, and procedures to gain an understanding of the committee's membership, responsibilities, and how it executes its duties. After reviewing these documents, examiners should meet with the Audit Committee chair to gain additional insights into committee responsibilities, processes, and engagement.

Evaluative questions and items to consider when examining Audit Committee structure, operations, and effectiveness include:

- ***Role Related to Internal Controls:*** **Is the Audit Committee's role sufficiently addressed in the internal control policy?** FCA Regulation 618.8430(d) requires the Audit Committee's role in providing oversight and review of the institution's internal controls to be addressed in the internal control policy. At a minimum, this must address the required role in FCA Regulation 620.30(d)(3) to oversee the institution's system of internal controls (including any internal audit functions) relating to preparation of financial reports.

- ***Charter:*** **Does the Audit Committee charter meet the requirements in FCA Regulation 620.30? Does it sufficiently identify any additional responsibilities the board has delegated to the committee?** A formal Audit Committee charter helps to define duties and

responsibilities. It also serves to remind committee members of their responsibilities and to familiarize new committee members with them. As a sound practice, the committee should review, update as warranted, and approve the charter annually. The charter should also be approved by the board and shared with auditors and reviewers.

- ***Membership:*** **Does the Audit Committee membership comply with regulatory requirements? Do members have the knowledge and skills to serve on the committee effectively?** FCA Regulations 620.30(a) and (b) identify specific membership criteria for composition and independence. A process should be in place to identify and document how each committee member meets the knowledge and independence criteria, including any financial expert(s). The board should strive to have members who best meet the knowledge criteria serve on the committee. Any designated financial expert(s) must serve on the Audit Committee. In addition to evaluating this process and verifying compliance with the regulatory requirements, examiners should evaluate whether committee members demonstrate the necessary knowledge and skills to carry out the committee's responsibilities effectively. This includes any additional board-delegated responsibilities, such as audit and review function oversight.

- ***Effectiveness:*** **Does the Audit Committee carry out its duties effectively and in compliance with its charter and FCA Regulations?** The Audit Committee needs to comply with requirements in its charter and FCA Regulation 620.30. However, when examining Audit Committee activities, it is equally important to confirm the committee is *effectively* carrying out its duties. A committee could comply with the regulations but not effectively perform its governance duties and responsibilities on behalf of the board. Documentation in board or committee materials, a discussion with committee members, and results from other examination procedures can evidence committee engagement and effectiveness. Examples of areas to consider regarding Audit Committee effectiveness include:

    - The quantity and quality of information is sufficient for the committee to effectively carry out its duties.

    - Committee members sufficiently question management and hold them accountable regarding issues under the committee's purview.

    - The committee completes sufficient review and due diligence before approving items requiring committee approval.

    - A formal onboarding process prepares new members to serve on the committee.

    - Committee size is appropriate for the institution's complexity and risk profile. An Audit Committee comprised of the full board may not devote sufficient time to thoroughly reviewing materials. A larger group may also hinder or impair individual members, including the financial expert, from asking sufficient questions. This could also apply if committee meetings have numerous management and staff in attendance.

    - There is an appropriate level of turnover in committee membership. A committee with limited turnover could be missing out on new or different perspectives from other board members. However, high turnover could hinder the committee's ability to be effective due to lack of consistency and experience on the committee.

- The committee completes self-evaluations that provide insight into the committee's strengths and weaknesses, developmental needs, and potential changes to membership.

- The committee receives quality, ongoing training. Training can be from various sources (e.g., consultant, conferences, management) but should be relevant to the committee's needs (e.g., accounting, finance, financial reporting).

- ***Additional Responsibilities*: If the board delegated other responsibilities to the committee, has the committee carried them out effectively?** As noted above, additional responsibilities beyond those required by FCA Regulations should be outlined in the Audit Committee charter. Frequently, the Audit Committee is responsible for direct oversight of the audit and review programs (beyond financial reporting). This may include engaging and overseeing auditors and reviewers, approving the audit plan and risk assessment, receiving audit and review reports, and ensuring corrective action in response to audit and review findings. Examiners should evaluate whether the Audit Committee has effectively carried out all significant board-delegated governance responsibilities.

Refer to the following documents for additional guidance and information:

- FCA's *Audit Committee* workpaper (see Part 3 of the Examination Manual).
- The *Audit Committees* section in FCA's FAQs about Governance Changes in 2006.
- The *Board Committees* section in FCA's The Director's Role.
- FCA Regulation 630.6(a) for requirements specific to the Federal Farm Credit Banks Funding Corporation that require it to have a System Audit Committee.

2. Policy & Procedures:

Evaluate the adequacy of guidance for carrying out the audit and review function.

Guidance:

FCA Regulations require institutions to have an internal control policy that includes adoption of internal audit procedures. These policies and procedures should include guidance and standards that address the key audit and review functions and activities. Evaluative questions and items to consider when examining audit and review policy and procedures include:

- ***Regulatory Compliance:* Does the institution have audit and review policy and procedures as required by FCA Regulations?** FCA Regulation 618.8430(b) requires adoption of internal audit procedures that evidence responsibilities for review and maintenance of comprehensive and effective internal controls. FCA Regulation 618.8430(c) requires policy guidance that provides direction for operating a program to review and assess the institution's assets. Policies must include standards to address the administration of this program (refer to the regulation for the specific standards that must be included). If examiners identify any significant gaps in an institution's audit and review of internal controls or assets, they should assess whether the policy and procedural guidance required by this regulation was deficient.

- ***Content:* Does the institution sufficiently outline the processes, guidelines, and responsibilities related to audit and review functions?** The level of guidance should be based on the institution's complexity, scope of activities, and risk profile, and be appropriate

for the type of internal audit and review function at the institution (internally staffed or outsourced). (IIA Standard 2040) An institution might provide this guidance within institution policies, procedures, an internal audit and review manual, or an internal audit department charter. Regardless of the format, effective audit and review programs should have guidance that addresses the following:

- *Purpose, Authorities, and Responsibilities* – Guidance should define the internal audit and review function's purpose, authorities, and responsibilities, including the use of internal audit to perform non-audit activities. It should also authorize access to relevant records, personnel, and physical properties. (IIA Standard 1000)

- *Professional Standards* – Guidance should identify any professional standards the institution has adopted for carrying out an ethical and effective audit and review program. It is appropriate for all institutions, and highly recommended for more complex institutions, to consider adopting the IIA's International Professional Practice Framework (IPPF), even when the internal audit function is largely outsourced.

- *Risk Assessment* – Guidance should address developing and using risk assessment tools, including the risk scoring system to be used and the range of scores (e.g., low, medium, and high; or a numerical sequence, such as 1 through 5). The guidance should typically include the following (refer to the *Planning* procedure for additional information):

    - Identification of who will be involved in developing the risk assessment and evaluating major risk areas.
    - What needs to be included in the risk assessment (e.g., all potential auditable areas).
    - Approach for overriding risk assessments.
    - Timing of risk assessments for each department or activity.
    - Minimum documentation required to support scoring or assessment decisions.

- *Audit Planning* – Guidance should outline the steps involved in creating the annual audit and review plan, identify the parties to be involved, and address the approval process. The guidance should identify the process for establishing audit and review scope and frequency, including prioritization of auditable areas and frequency based on the risk assessment results. Guidance should also identify how subsequent changes to the plan, if needed, will be completed and approved. This should include how any deferred auditable areas will be addressed in the next audit cycle. Refer to the *Planning* procedure for additional information.

- *Staffing and Engagements* – Guidance should address the process for staffing audit and review programs with qualified personnel. This includes addressing areas such as independence, objectivity, and qualification standards. Additionally, guidance should outline the processes and expectations for engagement contracts with outsourced staff for internal audits and reviews, if applicable. Guidance regarding outsourcing may be included elsewhere (e.g., as part of the institution's third-party risk management processes). Refer to the *Staffing* procedure below and the *Third-Party Risk Management* procedure in the *Corporate Governance* Examination Manual topic for additional information.

- *Documentation* – Guidance should outline the practices and processes for conducting fieldwork and testing, completing work programs, and maintaining workpaper documentation. (IIA Standard 2240) Documentation guidelines should ensure there is sufficient support for the work performed and resulting conclusions, and address workpaper filing and retention expectations. Additional details should be provided when automated audit management systems are in use, including use of templates, audit workflow design, user access levels, security, and backup of those systems. For institutions that primarily outsource the audit and review function, less guidance may be appropriate as the audits are typically conducted in accordance with the auditor's practices and processes, which should be outlined in the audit contract.

- *Reporting and Corrective Actions* – Guidance should outline the standard contents of audit reports and how and when audit and review findings will be reported to the board (or Audit Committee, if so delegated). Additionally, guidance should outline how the board will monitor overall progress of the audit and review program. Refer to the *Reporting Processes* procedure for additional information. The guidance should also detail how the board will ensure timely corrective action is taken to address findings. This should include expectations for management responses and audit and review followup on the adequacy of corrective actions. Refer to the *Corrective Action Processes* procedure in the *Corporate Governance* Examination Manual topic for additional information.

3. Staffing:

Evaluate the qualifications, training, and independence of audit and review program staff, and assess the adequacy of program staffing relative to institution complexity and risk.

Guidance:

The board and management should consider many variables, including the IIA's 3 lines model, when staffing audit and review programs and determining whether to use internal or outsourced staff. Regardless of the approach used, staff needs to be independent, objective, and have the necessary competencies to successfully implement the programs in a proficient and professional manner. In addition, the institution needs to ensure sufficient staffing to complete audit and review activities in a timely and effective manner. The institution may consider co-sourcing or outsourcing to help provide the needed audit and review resources. Inadequate or unqualified staffing can be one of the greatest obstacles to high-quality audit and review programs.

Evaluative questions and items to consider when examining audit and review staffing include:

- ***Audit and Review Program Structure:*** **Is the approach to structuring and staffing the audit and review programs appropriate for the institution?** The board (or Audit Committee, if so delegated) should consider factors such as the nature of the areas to be audited and scope of work to be performed, along with the complexity and risk profile of the institution, when determining the best staffing approach. As the complexity of an institution grows, the board should reevaluate the needs of the internal audit and review function to ensure it remains effective and fully staffed to carry out its responsibilities. (IIA Standard 2030) The primary approaches to staffing and structuring the audit and review function include in-house, outsourcing, and some combination of the two (i.e., co-sourcing). In-house audit and review programs are staffed with institution employees, whereas outsourced programs use outside

parties to complete audit and review activities (under the oversight of an in-house audit coordinator to facilitate the process). Co-sourcing arrangements involve engaging outside parties to supplement the use of in-house staff, with the engagements typically being overseen by the internal audit and review department staff. Each approach has advantages and disadvantages that should be considered when determining the audit and review program structure. When the institution does not have an internal audit and review department, the board's involvement in directing and operating the audit and review function may increase. It is critical for the board to ensure that no matter what structure is implemented, the auditors and reviewers have the necessary skills, credentials (e.g., Certified Internal Auditor, Certified Public Accountant), independence, and objectivity.

- ***Audit and Review Leadership:*** **Has the board (or Audit Committee, if so delegated) appropriately staffed the chief audit executive (CAE) or audit coordinator position?** The board, with management assistance, should recruit and retain a CAE or audit coordinator. The CAE or audit coordinator needs to have the necessary skills, independence, and objectivity to carry out their duties as discussed below. Note: FCA's FAQs About Governance Changes in 2006 (question #56) states the Audit Committee does not have regulatory authority to hire or fire internal audit staff, but the board can delegate this to the committee. The following are specific considerations for the CAE and audit coordinator positions:

    - *Chief Audit Executive* – This is typically a full-time employee of the institution. The specific job title of the CAE may vary across institutions. For example, institutions may use titles such as chief auditor and reviewer, director of internal audit, or chief audit director. This person is responsible for managing the internal audit and review function, including internal audit and review staff and outsourced engagements. (IIA Standard 2000). It is also beneficial to consider the CAE as a key position in succession planning.

    - *Audit Coordinator* – When an institution does not have a CAE on staff, these duties are completed by another employee as a collateral duty. The board should assign this duty to someone who understands the function and has no responsibility for operating the system of internal controls. Duties of an audit coordinator often include coordinating the risk assessment and audit planning, managing outsourced engagements, reviewing workpapers from outsourced engagements, tracking corrective action progress, communicating with the Audit Committee, etc.

- ***Competencies:*** **Do in-house auditors and reviewers, including the CAE and audit coordinator, have the skills and competencies to perform their duties?** In-house auditors and reviewers, including the CAE and audit coordinator, need to possess the necessary skills and competencies to perform their duties. Specifically, the CAE and audit and review staff should have the necessary skills and competencies and exercise due professional care to effectively carry out the audit function. (IIA Standards 1200, 1210, and 1220) Additionally, auditors and reviewers need to maintain their skills through continuing professional development. (IIA Standard 1230) While a CAE and in-house staff need to possess auditing skills, an audit coordinator should possess some knowledge in the area. For example, an audit coordinator should have a general knowledge of internal audit and review functions, including audit planning, scoping, engagement contracts, reporting, and corrective actions. Examiners can evaluate audit and review staff competencies by reviewing items such as:

- Resumes, including educational background, work experience, and involvement in professional organizations.
- Certifications, such as a Certified Internal Auditor, Certified Public Accountant, or Certified Information Systems Auditor.
- Commitment to continuing education through participation in courses sponsored by industry groups or through in-house training programs.
- Application of auditing techniques, such as internal control questionnaires and risk and control matrices (RACM), testing (including use of statistical sampling), flowcharting, electronic workpapers, and use of computer systems or programs to sample data.
- Job descriptions and performance evaluations.
- The quality of work performed and the ability to effectively communicate the results of that work.

- ***Independence and Objectivity:*** **Does the board (or Audit Committee, if so delegated) ensure the independence and objectivity of in-house auditors and reviewers?** The board has a fiduciary responsibility to ensure appropriate independence and objectivity in the audit and review program. The board should position internal audit staff so they can perform their duties with impartiality and not be unduly influenced by managers of day-to-day operations. Additionally, the board should ensure the person assigned to manage the audit and review function does not have responsibilities for developing or operating a system of internal controls or actually performing operational duties or activities. Specifically, the CAE or audit coordinator should be a member of management and be positioned in the organization to ensure independence, objectivity, and organizational stature. While the CAE or audit coordinator serves the combined needs of the board and management, to ensure independence, the board needs to retain oversight of the CAE or audit coordinator with a functional reporting relationship. The CAE or audit coordinator may report administratively to management (ideally the chief executive officer); however, the board should retain the authority for hiring and dismissal of the CAE or audit coordinator and be involved in the performance evaluation process. (IIA Standards 1100, 1110, and 1111) The objective is not to preclude management's involvement; rather, it is to ensure the board's involvement to facilitate an independent and objective audit and review function. The board should take measures to confirm that any administrative reporting relationships do not impair independence or unduly influence the person's work. Examples of things that may evidence internal audit independence and objectivity include the following:
  - Executive sessions with the board (or Audit Committee, if so delegated) should occur with those carrying out the audit and review function. This will afford auditors the opportunity to meet without management present and mitigate the risk of undue influence.
  - There should be no inappropriate restrictions placed on the audit and review staff, including scheduling or budgetary restraints imposed by management.
  - The board should be involved in determining the compensation structure of the audit department. Incentives for auditors should not be linked to audit results. A

separate incentive structure should be considered for audit and review staff to aid in objectivity of the audit function.

- ***Outsourcing:*** **Does the institution adequately manage its outsourced audit and review resources?** The institution may contract audit and review work with outside professionals to gain operational efficiencies or expertise. For example, the institution may use outsourcing when the internal staff members lack the expertise needed in specialized areas or when internal resources are insufficient. However, the institution needs to maintain ownership of the audit function and actively oversee outsourced activities. (IIA Standard 2070) A CAE or audit coordinator can be responsible for overseeing these resources, but the board (or Audit Committee, if so delegated) remains accountable for ensuring any outsourced activities are competently managed. Refer to the *Third-Party Risk Management* procedure in the *Corporate Governance* Examination Manual topic for information on examining an institution's outsourcing processes. The following are additional considerations when evaluating internal audit and review outsourcing:

    - Due to the nature of outsourcing, the institution should perform sufficient due diligence to verify vendor competence before entering the outsourcing arrangement. This includes verifying the vendor adheres to professional standards, such as those communicated by the AICPA or IIA. This may also include requesting resumes or quality assurance reviews to assist in selecting the appropriate vendor to conduct specific audits and reviews.

    - The board should periodically evaluate the quality of the vendor's work and ongoing competency, and consider changing or rotating outsourced auditors and reviewers, if necessary.

    - Engagement contracts should be in place prior to starting the work. The board should review and approve engagement contracts and discuss the terms with the party being engaged, as needed. Items that should typically be addressed in an audit or review engagement contract include:

        - Details on the scope, which should be commensurate with the scope in the approved audit and review plan.

        - Time period and other engagement terms that are consistent with the established scope and frequency in the plan and adequate to meet audit or review objectives and assist the board in meeting its fiduciary responsibilities.

        - Details on who will perform the activities (if different from the original proposal) and their qualifications.

        - The framework, principles, or body of standards under which the activity is to be completed (e.g., IIA or AICPA).

        - Expectations on access to workpapers prepared to support the audit report.

        - Defined lines of communications between the institution and the engaged auditors.

- If the institution is outsourcing its audit or review function, the board should remain responsible for reviewing and understanding the engagement, including the scope and work performed. Relying on managers in the first or second line (e.g., chief financial officer, chief operating officer, or chief executive officer) to complete this responsibility could present independence and objectivity issues. The CAE or an independent audit coordinator should ensure that work performed agrees with the scope of the engagement. This may include reviewing audit workpapers to ensure the depth and breadth of work completed was consistent with the engagement letter, audit plan, and the board's expectations.

- ***Internal Audit and Review Program Assessments:*** **Does the institution conduct appropriate assessments of the internal audit and review program?** Internal and external assessments help ensure internal audit and review processes and activities are ethical, effective, and add value to the institution. Regardless of the institution's internal audit and review program structure, assessments should be conducted periodically, as outlined below:

  - For institutions that have adopted the IIA standards, the internal audit and review department needs to maintain a Quality Assurance and Improvement Program (QAIP). (IIA Standards 1300, 1310, 1311, 1312, 1320, 1321, and 1322) The QAIP includes both internal and external assessments of program activities and helps the internal audit and review department establish benchmarks and metrics that align with and meet the requirements of the IIA standards. External assessments are required at least once every 5 years while internal assessments should be conducted periodically. A QAIP helps ensure alignment with IIA standards and can improve the productivity, expertise, and effectiveness of the internal audit and review function. Outsourced providers that adhere to the IIA standards should have a QAIP in place. The board should consider third-party providers that conform with IIA standards or similar frameworks (e.g., AICPA) when engaging audit and review resources. If the outsourced provider does not conform to an auditing framework, the board and management need to ensure the quality of the provider's work.

  - For institutions that have not adopted the IIA standards, we expect them to periodically (every 3-5 years) arrange for an external assessment of the audit and review program's independence and effectiveness. This assessment can be completed in numerous ways (e.g., partner with other System institutions or hire a third-party).

4. Planning:

Evaluate the adequacy and implementation of the audit and review plan(s), including the risk assessment process, to ensure all material operational areas and risks are sufficiently addressed.

Guidance:

The audit and review planning process is essential to maintaining effective, risk-based audit and review programs. Key aspects of the planning process include conducting a risk assessment and developing an audit and review plan. Risk assessment involves identifying and evaluating the quantity of institutional risks and the quality of controls over those risks. Results of the risk assessment should guide the development of the audit and review plan. The risk assessment and audit plan should aim to provide the board and management with reasonable assurance of adequate audit and review coverage in all high-risk and significant operational areas, with rotational coverage

of lower risk areas.

Evaluative questions and items to consider when examining audit and review planning include:

- ***Board Involvement:*** **Does the board (or Audit Committee, if so delegated) provide effective review and oversight of the risk assessment and audit and review plan?** The board should have a thorough understanding of the institution's audit and review needs. For example, the board should be sufficiently involved in the risk assessment process to understand the institution's risk profile, particularly before approving the audit and review plan and making strategic decisions. This can be accomplished by board questionnaires or surveys, or by soliciting input from management, auditors, reviewers, and others during the risk assessment and audit planning processes. If the internal audit and review function is outsourced, the board should develop the risk assessment or work with the audit coordinator to develop it. The board should also review and approve the audit and review plan at least annually. (IIA Standard 2020) This would include the internal audit and review cycles, schedules, scope, and resource allocation for each area to be audited. The following additional items warrant board involvement:
    - The board should be apprised of risk assessment adjustments throughout the year.
    - The board should remain involved in key audit scope discussions during the annual planning process and throughout the audit cycle. In some cases, the specific audit or review scope may be determined closer to the actual activity date rather than during the annual planning process. When this occurs, the board should be provided an opportunity to review and discuss the scope prior to the work commencing. For institutions that have an internal audit department, scope review and approval processes may vary depending on the independence and depth of the audit department.
    - The board should monitor audit and review plan implementation on an ongoing basis and approve any material changes to the plan.
- ***Risk Assessment:*** **Does the risk assessment adequately address all significant business activities? Are the risks appropriately identified and prioritized? Is the risk assessment completed per institution guidelines?** The risk assessment process begins by defining the audit universe, which includes a comprehensive listing of the institution's operational functions and significant business activities (e.g., current and prospective businesses, product lines, and services). The audit universe needs to have sufficient granularity to prevent audit and review coverage gaps. The risk assessment needs to evaluate current and emerging risks and controls associated with the functions and activities identified in the audit universe. Risk assessments should also address how internal and external risk factors potentially impact each auditable area. Risk assessments that appear comprehensive but have not changed from the previous year may not include a new business line or emerging risk. The risk assessment process should have a defined approach to measuring risk across the audit universe. A risk scoring system should be developed which helps to prioritize risk and direct audit and review frequency. Institution guidelines and procedures should be followed when conducting the risk assessment to provide consistent and accurate results. Refer to the *Policy & Procedures* procedure for additional information. The following are additional considerations when evaluating an institution's risk assessment:

- The institution should consider the possible impact of the various risks on achieving strategic business objectives and the likelihood of their occurrence. From there, the institution's risk profile can be developed. The following are examples of factors institutions should consider when conducting a risk assessment:
    - Any changes or additions to the institution's operations or risk profile.
    - Conclusions from previous audit and review activities.
    - Regulatory requirements and guidance, including any new or revised regulations or FCA National Oversight Plan topics.
    - The nature of the operational processes and related assets and liabilities within each potential audit area.
    - The existence and effectiveness of applicable policies, procedures, and internal controls (e.g., separation of duties, management reviews, reporting processes). Areas with weak or limited controls would typically require more frequent, in-depth testing.
    - The potential materiality of errors, omissions, and irregularities.
    - The potential for fraud and adequacy of anti-fraud controls.
- Risk assessment approaches may vary depending on factors such as the institution's complexity, risk profile, scope of activities, staff capabilities, quality of control functions, and technology used.
- Internal audit should complete its own risk assessment while considering information from risk assessments completed by management. Conducting the audit risk assessment generally involves using prior audit and review results, interviewing key process leaders, obtaining board and management input, and coordinating with other risk management groups.
- Risk assessment results should guide audit and review plan development, the audit schedule, and the scope and objectives of individual audits and reviews. The risk assessments should enable the institution to focus audits and reviews on the areas of greatest risk and set priorities.
- Risk assessments should be completed at least annually and updated as needed when risks change. For example, the risk assessment should be updated if the institution experiences significant growth, new products are introduced, processes are revised, staff turnover occurs in key roles or is above normal, activities shift, or laws and regulations change. Additionally, as part of the risk assessment process, the audit universe should be reviewed for updates at least annually. For example, there may be new or obsolete operational areas to consider.

- ***Audit and Review Plan:*** **Does the annual audit and review plan adequately cover all auditable areas and is it consistent with risk assessment results? Is the planning process completed per institution guidelines?** The audit and review plan should cover all auditable areas in the audit universe, be based on the results of the risk assessment, and be prepared in accordance with institution guidelines. It should address the risks identified in the risk

assessment, especially those identified as high risk, and incorporate input from the board and management. (IIA Standard 2010) The risk assessment results should help establish audit and review prioritization and guide the scope and frequency. For example, potentially high-risk areas normally warrant more frequent review than low-risk areas. However, individual judgment and circumstances at each institution will factor into the audit cycle length and scope. The plan should describe goals, schedules, staffing, and reporting, and be prepared in accordance with the institution's audit and review program policy and procedures. If possible, the plan should include an element of surprise when conducting some audit and review activities. It should also address the following specific items:

- Summary of the risk assessment results for each auditable area or business activity identified in the audit universe.
- Individual audit or review objectives and scope. Typically, the scope in the annual audit and review plan is high level and focuses on what areas are to be audited, rather than the specific steps to be completed in those audits. The plan should provide enough information to understand the general expectations of what will be covered in each audit and review. A plan might indicate an area will be audited but, due to lack of detail, it is unclear what part of that area will be audited, resulting in audit coverage gaps. For example, if the plan says to evaluate the YBS program with no additional information, it could be interpreted as either transaction testing of YBS coding or an operational audit of YBS processes, controls, reporting, etc.
- The timing and frequency of planned audit and review work, including a schedule of past, current, and future activities. A matrix or similar method should be used to display the frequency and schedule for each area. It should cover a 3-year range or longer, with actual information from prior years. With this information, the board can appropriately monitor audit and review coverage and ensure audit cycles are not open-ended or pushed out indefinitely.
- A resource budget that addresses staff days needed and other audit and review costs, including outsourced engagement fees.

5. Reporting Processes:

Evaluate the adequacy of processes for reporting audit and review activities and results.

Guidance:

Reporting processes should provide the board assurance that material weaknesses, including their underlying causes, are being identified and communicated in a timely manner. To accomplish this, reporting processes should ensure that reports clearly communicate the audit or review scope, findings, conclusions, and recommendations to appropriate parties, and are distributed as soon as practical after completing the related work. Reporting processes should also ensure independence and objectivity are maintained, the audit and review plan is being implemented.

Evaluative questions and items to consider when examining audit and review reporting processes include:

- ***Report Quality, Content, and Timeliness:*** **Are processes and expectations on audit and review report quality, content, and timeliness sufficient?** The institution should establish

audit and review reporting processes to identify the board's expectations on report quality, content, and timeliness. These processes should address items such as:

- Standards for what to include in audit and review reports. Reports should be complete, accurate, and provide sufficient detail on the purpose, objectives, scope, results, conclusions, and recommendations. (IIA Standards 2330, 2400, 2410, 2420, 2440, and 2450)

- Expectations for audit's evaluation of management's responses and corrective actions to address prior findings and determine if follow-up testing is necessary. (IIA Standard 2500)

- Standards for time frames from conclusion of fieldwork, to obtaining management responses (if included in report), to publication of the final report. (IIA Standard 2420)

- Expectations for timeliness in providing audit and review reports to the board. Reports should be given to the board in a reasonable time frame after publication so the information remains relevant. (IIA Standards 2420 and 2440)

- Expectations for when material audit findings should be more quickly communicated to the board and management. Material findings and conclusions should be communicated soon after they are identified, rather than waiting until the final report is issued. (IIA Standard 2440)

- ***Independence:*** **Do auditors and reviewers report directly to the board (or Audit Committee, if so delegated)?** FCA Regulation 620.30(d)(2) requires an institution's external auditor to report directly to the Audit Committee. While the regulation is specific to the external auditor engaged to audit the institution's financial statements, internal audit and review reporting should follow a similar approach and be directly to the board (or Audit Committee, if so delegated). (IIA Standards 2060 and 2440)

  - Direct reporting will help support independence and objectivity for the audit and review process. Management can, and should, be provided audit and review reports; however, a direct line of reporting and communication with the board must be maintained. Management must not be able to control the message or exert undue influence on the auditor's or reviewer's ability to provide the message to the board.

  - As a sound business practice, the auditor or reviewer who completed the work, not management, should present oral reports to the board. This is important as it enables the board to ask the auditor or reviewer questions on specific findings, recommendations, and management action plans to address concerns.

  - As a sound business practice, the board should have ongoing communications with the CAE or audit coordinator. This helps the board better understand audit and review programs and allows for any issues or concerns to be addressed timely.

- ***Reporting on Audit Progress:*** **Are processes in place to ensure the board is provided the necessary information to effectively monitor the audit and review programs? Does the board have sufficient processes to track progress on completing planned audits and reviews in accordance with the approved plan?** Processes should ensure that audit and

review reports and other audit-related information submitted regularly to the board are sufficient for effectively monitoring internal audit and review performance and progress toward meeting approved plans and schedules. The board should receive updates on audit and review plan progress regularly throughout the year (e.g., quarterly), in accordance with established policy. For example, reporting expectations should address comparing actual work performed to the approved plan, identifying significant plan variances, and explaining any material changes in scope.

Refer to the *Corrective Action Processes* procedure in the *Corporate Governance* Examination Manual topic for examining corrective action processes and general reporting in response to corrective actions from internal and external audits, reviews, and examinations.

6. Effectiveness & Reliability of Audits/Reviews:

Determine the effectiveness and reliability of audit and review activities based on an evaluation of individual audits/reviews and any related FCA transaction testing.

Guidance:

Institutions typically conduct multiple audits and reviews throughout the year. Examples include internal credit reviews, internal operations reviews, appraisal reviews, information technology audits, and other financial or operational audits and reviews. FCA evaluates these individual audits and reviews as part of examining the applicable topical area.

There is an *Audit* procedure within each applicable Examination Manual topic that is specifically tailored to examining audit and review program effectiveness and reliability. Conclusions on audit and review program effectiveness and reliability are based on a rollup of the results from these individual *Audit* procedures. Examiners should consider factors such as the sample size (how many of the institution's audit and reviews FCA examined) and who completed the audit and review work that was evaluated (an institution may have multiple staff or vendors completing the work). This is important to ensure examination conclusions are appropriate relative to the examination work completed.

In addition, the following are specific evaluative questions and items to consider when rolling up and summarizing examination work on the effectiveness and reliability of audits and reviews:

- ***Audit Coverage:*** **Is there sufficient audit and review coverage?** Audit or review coverage and frequency in the areas examined should be appropriate relative to risks, changes in the operating environment, regulatory requirements, and periodic testing needs. Coverage should also be consistent with the institution's risk assessment results and annual audit plan.

- ***Scope and Depth:*** **Are audit and review scope and depth sufficient and consistent with approved plans?** The scope and depth of work should cover the primary processes and controls within the area being audited or reviewed and be sufficient to determine if internal controls are functioning as intended and regulatory requirements are met. The scope and depth of coverage in each audit and review should also be documented and consistent with the approved audit or review plan and engagement contract (if applicable). Audit and review workpapers should be examined to verify the actual scope and depth of work performed. The workpapers may indicate the scope and depth deviated from what was identified (or implied) in the plan. For example, the workpapers may indicate the work performed was limited to evaluating the existence of policies and procedures and didn't include reviewing

other controls, such as training or reporting, or testing compliance with regulations or institution guidance. If the work deviated from the original planned scope, internal audit should notify the board (or Audit Committee, if so delegated) of the reasons for the change.

- ***Reliability of Results:*** **Are audit and review results reliable?** It is important to understand the scope and depth of each individual audit and review being examined, as discussed above, when evaluating audit and review reliability. With this understanding, the following are key considerations when evaluating the reliability of audit and review results:

    - *FCA Testing* – FCA typically evaluates the reliability of internal audit and review work by comparing the results conveyed in the internal audit and review report to FCA's examination results. The comparison often includes FCA testing transactions that were covered in the internal audit or review (transactions are often loans or loan applications, but may include other types of transactional activity, as well). Examiners should also obtain and review the audit or review workpapers to more thoroughly understand and evaluate the work completed. This can be especially important if the audit or review report is not sufficiently detailed or FCA's examination work and testing identifies potential concerns. Auditors and reviewers complete line sheets, flowcharts, control matrices, standard work programs, workpaper forms, or other relevant audit evidence when conducting and supporting their work. (IIA Standards 2240, 2300, 2310, and 2320) Workpapers should adequately document the work performed and support the final report. If FCA identifies weaknesses that were not identified in the audit or review, the cause for any discrepancy should be determined. Examiners should consider the significance of such discrepancies across all the individual audits and reviews examined when determining overall reliability of audit and review results.

    - *Audit/Review Staffing* – Whether internal or outsourced, auditors and reviewers conducting the work need to be qualified, independent, and objective to ensure reliable results. They should have the right mix of knowledge, skills, and other competencies needed to perform the work. (IIA Standard 2230) Additionally, auditors and reviewers need to be independent of the activities they audit so they can carry out their work freely and objectively. (IIA Standards 1100, 1112, 1120, and 1130) For example, audit and review staff should not be involved in developing and installing procedures, preparing records, operating a system of internal controls, or engaging in any other activity that they would normally review. Examiners should evaluate the staffing on the individual audits and reviews being examined as part of determining the reliability of audit and review results.

    - *Institution Review of Work Performed* – The institution should complete an independent review of the workpapers to ensure audit and review objectives and scope were met and the results and conclusions were reliable and supported. (IIA Standard 2340) Examples could include a supervisory review of in-house audit work by the CAE or other audit staff, or a review of outsourced work by the CAE or audit coordinator. Examiners should consider whether the institution completed these reviews, and if any concerns were identified, when concluding on audit and review reliability.

- ***Reports:*** **Do audit and review reports sufficiently communicate work performed, results, and recommendations?** Audit and review reports should be prepared and communicated in accordance with the institution's guidelines. They should be accurate, concise, supported,

and timely in communicating the audit and review objectives, scope, results, conclusions, and recommendations. (IIA Standards 2330, 2400, 2410, 2420, 2440, and 2450) An executive summary or overview should be included to provide the board with a general conclusion on results. Results and conclusions should be supported by convincing evidence and persuasive arguments (condition, criteria, cause, and effect). Results in the workpapers should align with report conclusions. Recommendations should be realistic and reasonable given the institution's complexity and risk, with material and higher-risk issues clearly prioritized. Reports should tell the board and management whether the institution adheres to policies, procedures, and applicable laws or regulations, and whether operating processes and internal controls are effective. Reports should also address potential vulnerabilities to fraud, as applicable.

- ***Corrective Action:*** **Are management responses to audits and reviews reasonable, complete, and timely? Have corrective actions been effective?** Audits and reviews are only effective if corrective action is taken to remedy the weaknesses identified. As such, reasonable, complete, and timely management responses are needed for the individual audit and review reports. Management commitments and agreements or any areas of disagreement should be documented in the report or in a separate memo or tracking system. (IIA Standards 2500 and 2600) If corrective actions are not resolving the issues or concerns in a timely manner, examiners should further investigate the reasons. For example, this could indicate that audits and reviews are not sufficiently identifying the underlying causes or materiality of weaknesses, sufficient resources are not being directed toward corrective actions, or weaknesses exist in the institution's corrective action process, including board oversight of the process.