EM-31.1

Category: **Board & Management Operations**
Topic: **Direction & Control of Operations**
Published: 1/17/2025

Overview

The *Direction & Control of Operations* topic provides guidance on evaluating the effectiveness of a Farm Credit System (System) institution's board and management in governing operations and risk management activities in a responsible and ethical manner. Direction and control of operations is a key component of board and management operations. Direction and control speaks to the guidance and practices for establishing the institution's risk management, internal control framework, and other governance processes. A comprehensive evaluation of board and management direction and control activities should address both regulatory compliance and overall effectiveness. We address other important components of direction and control of operations (e.g., business planning processes, audit and review programs, director elections, human capital management, business continuity, standards of conduct practices) as stand-alone Examination Manual topics.

Examination Procedures and Guidance

General

1. Enterprise Risk Management:

Evaluate the use of an enterprise risk management program and related processes to identify and manage risks from an institution-wide perspective.

Guidance:

Enterprise risk management (ERM) programs are prudent business practices that provide a disciplined approach to identify and manage risk. ERM applies an institution-wide, integrated approach where all levels of management and staff play a part in identifying and managing risks within established parameters. ERM builds on an institution's routine risk management practices by integrating them with strategy, planning, and day-to-day decision making. ERM helps institutions achieve performance goals and positive outcomes by providing for better understanding, management, and reporting of risk.

An ERM program involves a progressive process that can take several years to implement and refine. It is important for the board and management to decide early in the process what they hope to achieve from an ERM initiative. They should use this information to determine the scope of the ERM program. Commonly, different divisions or teams may have already developed their own risk management practices and it is unlikely that each used the same approach for identifying, evaluating, responding to, monitoring, and reporting risks. A transition or implementation plan is

typically needed to coordinate existing approaches into one ERM program across the institution. Once an ERM program has been implemented, it should continue to evolve over time as the business environment changes. The board and management should ensure it remains useful and current.

ERM initiatives can use various frameworks and approaches. A common ERM framework is the Committee of Sponsoring Organizations (COSO) ERM – Integrating with Strategy and Performance (June 2017 Executive Summary). The COSO Internal Control – Integrated Framework (May 2013 Executive Summary) is a complementary publication used as a framework for internal controls, including internal controls over financial reporting. These two COSO publications are distinct and have different focuses; neither supersedes the other. However, they connect and include similar concepts. The concepts applied should be adapted to the risk profile and complexity of the institution.

When applying the evaluative questions below, examiners should consider the maturity and capabilities of the ERM program and evaluate the program's effectiveness based on the institution's goals for the program and operational complexity. As the program matures and ERM is used in business decisions, examiners should increase the degree of scrutiny when examining ERM programs. The following guidance addresses the primary components of an effective ERM program.

Culture and Governance: An institution's culture and governance, together, provide the foundation for a successful ERM program. COSO defines culture as the attitudes, behaviors, and understanding of risk that influence the decisions of management and staff and reflect the mission, vision, and core values of the institution. Culture can affect how risk is identified, assessed, and responded to, beginning with strategy setting through execution and performance. Risk culture can be measured by determining the institution's risk maturity. Institutions can be in different risk maturity phases, which typically evolve over time (see the Institute of Internal Auditors (IIA) risk maturity levels for an example). Governance is the combination of processes and structure implemented by the board to inform, direct, manage, and monitor institution activities toward achieving objectives. Evaluative questions and items to consider when examining culture and governance include:

- ***Risk Culture:*** **Has the board and senior management set and communicated clear expectations and values that describe the desired risk culture?** Risk culture helps determine whether there is genuine buy-in at all levels to address risks and opportunities arising from event uncertainty. A well-defined risk culture stresses the importance of managing risk and encourages transparent and timely flow of risk information. This informs personnel about the boundaries within which they can operate and helps define the institution's risk appetite. When the risk culture is defined, understood, and embraced by management and staff, the institution is better positioned to effectively recognize and manage risk. Therefore, the risk culture needs to be communicated throughout the institution. Formal ways to communicate a risk culture include risk appetite statements, risk metrics and thresholds, dashboards, reporting, training, memos, conferences, policies, and procedures. It is also important for the board and management to reinforce the established risk culture, not only with words, but with everyday actions.

- ***Policies and Procedures:*** **Do policies and procedures provide adequate guidance and direction on ERM?** The board and management should develop an ERM policy and related procedures. As outlined in The Director's Role, the board is responsible for overseeing significant institutional programs and activities by setting policy. The policy should address the primary aspects of the ERM framework, such as the purpose and objectives; risk culture; oversight and governance expectations; key roles and responsibilities; authorities delegated;

description of core ERM processes and strategies (risk tolerances, risk assessment and controls, review activities); and reporting requirements. Management should develop procedures to implement the board policy and provide guidance on the significant processes and protocols for ERM, including how changes will be made to the program as it evolves. Policy and procedural documentation should increase as the ERM program matures. ERM guidance should be periodically reviewed and updated, as needed.

- ***Roles and Responsibilities:*** **Are ERM-related roles and responsibilities appropriate and defined?** Identifying the roles and responsibilities around ERM is key to its success. ERM is an institution-wide, coordinated approach where all levels of management and staff have responsibilities. ERM tasks do not solely fall on the chief risk officer or senior management. Responsibility should be assigned for each element of ERM, including risk and event identification, risk management, monitoring, and reporting. Responsibilities should be clearly defined so each party understands the boundaries of their responsibilities and how their role fits into the overall risk and control structure. Outlined below are the widely accepted roles of each group that is potentially involved in ERM:

    - *The Board* – The board is responsible for setting the risk culture, approving policy, monitoring performance, and overseeing ERM, as well as contributing to and understanding the risk assessment and risk appetite. The board might also designate a board risk committee to oversee the ERM program.

    - *Senior Management* – The board typically delegates responsibility over the ERM program to the CEO. Senior managers are often part of the risk committee or group that focuses on managing risks in their areas of responsibility, promoting alignment with risk appetite, and supporting ERM. In the IIA's Three Lines Model, management's responsibility to achieve objectives comprises both first and second line roles. First line roles are most directly aligned with the day-to-day management of operations and risk while second line roles assist with monitoring and managing risk.

    - *Risk Officer or Management-Level Risk Committee* – ERM program administration typically falls under the second line in the IIA's Three Lines Model. In this second line, management should provide a forum for structured, cross-functional review, assessment, and management of the ERM program. This forum should include members from all operational areas of the institution and is typically comprised of management team members. Some institutions formalize this as a risk committee. If a risk officer is designated, the risk officer will likely head the ERM program and address risk issues in coordination with the senior management team. The risk officer should possess adequate knowledge, skills, and experience with ERM. The ERM policy or a committee charter should document authorities, responsibilities, operating parameters, and reporting requirements for a risk officer or risk committee. While a risk officer or risk committee is not required, having one of these is a sound business practice in a mature ERM program. The risk officer or risk committee would potentially:

        - Serve as the party responsible for ERM development and implementation.
        - Assist the board in formulating strategy and policy based on the risk culture and risk exposures.
        - Coordinate with the board in establishing risk appetite and risk tolerance levels.

- Review risk management activities and reports and compile risk assessment input.
- Create reports and provide recommendations to the board.
- Seek to improve and evolve management of key enterprise risks.
- Strive for continuous improvement of risk management systems.

- *Internal Auditor* – The board and management should determine the role internal audit plays with respect to ERM processes. Internal audit's role may vary; however, no matter the role, internal auditors need to maintain objectivity and independence and not be involved in making risk management decisions. Internal audit primarily serves in a third line role by providing assurances over ERM processes and evaluating ERM practices and program performance. Internal audit might serve in an advisory or consulting role, including championing, maintaining, facilitating, or coordinating ERM program and related activities. As risk maturity increases or if risk management professionals are hired, internal audit's role in championing ERM may be reduced. The board (or Audit Committee if so delegated) should approve any advisory or consulting roles. These roles should be clearly defined, with appropriate safeguards in place. Internal audit should not be responsible for managing risk or providing objective assurance on any part of the ERM program for which it is directly involved. For more information, see the IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management.

- *Other Institution Personnel* – This includes any staff responsible for executing ERM in accordance with established policies and procedures. These roles are part of the first line of defense. Employees should understand, accept, and implement ERM processes and cooperate with management. Staff should be trained to carry out established ERM duties.

- ***Internal Audit:*** **Is ERM appropriately considered in the audit universe and audited periodically?** ERM should be considered for audit periodically based on risk assessed, similar to other auditable areas. Refer to the *Audit* procedure for examining ERM audits.

Strategy and Objective Setting: ERM should be integrated with the institution's business plan strategies and objectives. The board often sets its risk appetite when determining its business strategies and objectives. If the risk associated with a specific objective is inconsistent with the institution's strategy, risk appetite, or risk capacity, the objective should be revised, an alternative strategy selected, or risk appetite revisited. Business objectives allow strategies to be put into practice and shape day-to-day operations and priorities. Progress on achieving strategies and objectives is measured by identifying performance measures and setting risk tolerance levels. Evaluative questions and items to consider when examining how ERM impacts business strategies and objectives include:

- ***Business Strategies and Objectives:*** **Does the ERM process accurately identify the risks associated with business strategies and objectives? Is the ERM program used to consider risks when setting business strategies and objectives?** Institutions conduct a general analysis of their business and identify objectives during strategic business planning. ERM should build off this analysis and consider the trends, events, relationships, and other factors that may influence, clarify, or change the institution's current and future business strategies and objectives. By integrating and involving ERM when setting strategies and objectives, the institution gains insight into the risk profile associated with business strategies and objectives.

- ***Risk Appetite:*** **Is a risk appetite(s) developed and maintained that is in line with business strategies and objectives?** It is common to develop strategies and risk appetite in parallel, refining each throughout objective setting. Risk appetite is defined as the types and amount of risk, on a broad level, the institution is willing to accept in pursuit of value. Risk appetite can also focus on desired goals or objectives to strive for risk optimization. The institution can have a singular, high-level risk appetite or multiple risk appetites applied to various risks or objectives. Either way, both top-down board leadership and bottom-up input should drive the development of risk appetite. Risk appetite is not a single, fixed concept and can change over time; therefore, it should be reviewed at least annually. The institution's existing risk profile, which is a composite view of risk assumed at a particular level or aspect of the institution, should be considered when developing the risk appetite. In addition to risk profile, the institution should consider its risk culture, ERM maturity, and risk capacity, which is the maximum amount of risk that an institution is able to absorb in the pursuit of its business strategies and objectives. Risk appetite can be expressed using general terms, such as high, moderate, and low, or with a quantitative approach such as financial results. As institutions become more experienced in ERM, risk appetite descriptions become more precise. Risk appetite should be documented in board policy, the business plan, or other ERM documents and communicated to appropriate parties.

- ***Performance Measures and Risk Tolerances:*** **Are ERM performance measures and risk tolerances established to measure achievement of business objectives?** Performance measures establish criteria to monitor achievement of objectives and should include both quantitative and qualitative metrics. Examples include credit ratios, capital ratios, earnings indicators, customer satisfaction, employee turnover, or underwriting exceptions. Risk tolerance is defined as the boundaries of acceptable variation in performance related to achieving business objectives. While risk appetite is broad, risk tolerance is tactical and operational, and represents the application of risk appetite to specific objectives. Performance measures and risk tolerances should be expressed in measurable units (preferably in the same units as business objectives). For example, a performance measure could be adverse assets-to-total loans (e.g., the business objective may be set at 3 percent and the risk tolerances could be no less than 2 percent and no greater than 5 percent). Risk tolerances and performance measures should map to the risk assessment and provide information as to where risk is in relation to risk appetite and meeting business objectives. Guidance should include processes to report when a performance measure exceeds the risk tolerance level and to determine actions needed to manage risk in alignment with risk appetite and target risk levels. Risk tolerances should be reviewed at least annually, but preferably on an ongoing basis to determine if adjustments are warranted. Performance measures should also be reviewed periodically to ensure they remain relevant and accurate measures of risk.

Performance: Performance involves identifying, assessing, prioritizing, and responding to risks that may affect the institution's ability to achieve its business strategies and objectives. The institution should consider risk appetite and prioritize risks according to their severity across the institution. The board and management should then select risk responses and monitor performance for change. ERM helps to develop an institution-wide (portfolio) view of the amount of risk the institution has assumed in the pursuit of strategies and institution-level business objectives. Evaluative questions and items to consider when examining performance include:

- ***Risk Assessment:*** **Has the institution developed a risk assessment process that identifies events and risks that would impact its ability to achieve objectives? Are those events and risks quantified using an established risk measurement system and criteria?** In the context of ERM, the risk assessment component is a continuous and iterative process that takes place throughout the institution. The risk assessment should consider both the inherent and residual risks of events. Inherent risk is the risk that exists in the absence of a risk response. Residual risk is the risk that remains after applying an actionable risk response. Target residual risk is the amount of risk that an institution prefers to assume in the pursuit of its business strategies and objectives. An ERM risk assessment is different than an internal audit risk assessment. The ERM risk assessment should be focused on identifying events and risks that may impact the achievement of strategies and objectives, whereas the internal audit risk assessment should be focused on identifying events and risks that may impact auditable areas. The ERM risk assessment process should consider activities such as business and financial planning, stress testing, risk surveys, industry analysis, prior audit results, and allowance for credit loss studies. The ERM risk assessment document should be formally updated annually to ensure changes in risks and objectives are being captured and evaluated. The ERM risk assessment should be the foundation for all ERM monitoring and reporting activities. While there may be many different systems in place to help assess risk, there should be one documented risk assessment for ERM that identifies, quantifies, and prioritizes risk. The risk assessment's key elements include:

    - *Identify Events and Risks* – A risk universe (sometimes referred to as a risk inventory) should be developed and documented during the ERM risk assessment process. A risk universe is a comprehensive listing of internal and external events and risks that could prevent the institution from achieving its business strategies or objectives. Additionally, an important part of identifying events and risks in ERM is identifying and understanding the underlying causes. The detail level of the risk assessment depends on the institution's needs and ERM maturity. Risks should be classified or categorized to group related risks; however, there is no universal classification of risk. As such, the institution can classify risk based on the nature of the risk (e.g., business risk versus non-business risk) or on business objectives or operational areas. Risks can be categorized by business unit or department, portfolio or market segment, event or type of risk (e.g., liquidity, reputational, operational, concentrations, market, compliance), or other areas. Developing a risk taxonomy (i.e., a grouping or categorization of risks) will make it easier to determine the appropriate risk response for the inherent risks and help position management to consider whether inherent or residual risks remain in alignment with the established risk appetite.

    - *Quantify Events and Risks* – The institution should have a documented risk measurement system and criteria to appropriately analyze and evaluate the events and risks and their underlying causes. For example, risk criteria could include vulnerability, velocity, volatility, interdependence, correlation, likelihood, or impact. The uncertainty of potential events is typically evaluated based on likelihood (possibility that an event will occur) and impact (effect from the event). This risk criteria will help determine the inherent risk rating of the identified risk. A *heat map* could be developed to quantify the risk level in a consistent format and help to develop a risk profile. The institution should remain mindful of its overall risk profile compared to total risk capacity while assessing individual risks. The risk

measurement system and criteria should be periodically reviewed for accuracy and effectiveness.

- ***Risk Priority:*** **Are risks appropriately prioritized?** Risks should be prioritized based on the severity of the risk rating, importance of the corresponding business objective, and risk appetite. Risk priority criteria should be established to consistently prioritize risk. Examples include adaptability, complexity, velocity, persistence, and recovery capability. The institution may assign a higher priority to those risks likely to approach or exceed the established risk tolerance or target risk level. A risk register can be used that documents a structured record of all risks identified in the risk universe. This register should include description, category, cause, performance measure, risk criteria, proposed responses, owners, and status. It should also incorporate the risk assessment ratings and identify the need for additional review, documentation, or action based on the risk level. Prioritizing risks will help demonstrate an institution-wide view of risk to highlight those that may not be sufficiently considered or that may be overly managed.

- ***Risk Responses:*** **Do risk responses align with risk appetite and help to manage potential risk exposures within established risk tolerances?** After assessing and prioritizing relevant risks, the institution should determine and document how it will respond to those risks from an enterprise-wide standpoint. A risk response refers to any action taken to modify the risk, whether to maximize the potential benefits or mitigate the negative effects. The typical risk responses are avoidance, reduction, sharing, and accepting. ERM requires risk to be considered from an institution-wide perspective. Risks in different units or portfolio segments may be within an individual area's risk tolerance; however, when aggregated, these risks might not align with the institution's risk appetite as a whole. In this case, additional or different risk responses are needed to bring risk back in alignment with the established risk appetite. On the other hand, one risk response might mitigate several risks or risk events. Even when risks fall within established risk tolerances, risk responses should be periodically reviewed for appropriateness. Risk responses should be prioritized based on the risk assessment results and identify the appropriate control activity, if applicable. Institutions can also benefit from developing a risk mitigation plan to record what is required to implement specific responses, as needed.

- ***Control Activities:*** **Do control activities align with risk appetite and help to manage potential risk exposures within established risk tolerances?** Once risk responses have been identified, control activities should be identified, documented, and implemented to ensure alignment with risk appetite and manage the potential risk within tolerances. The institution should already have control activities built into normal business operations through policies, procedures, systems, etc. However, an effective ERM process requires that control activities be identified and linked to the event or risk they are in place to manage. Control activities can vary between preventive, detective, directive, or corrective, and can be manual or automated. Similar to risk responses, a single control activity can address multiple risk responses and in other instances, multiple control activities may be needed for one risk response. Control activities help determine how much residual risk remains. To quantify residual risk, institutions should measure the control effectiveness of the inherent risk. Heat mapping, stress testing, or table-top discussion exercises are just some of the tools that can be used.

Review and Revision: Since ERM processes and risks change over time, management should determine whether the ERM program continues to be effective through documented review and

revision activities. Changes in business practices may lead to new or changed risks and affect key assumptions underpinning strategies. Identifying substantial changes, evaluating their effects, and responding to the changes are iterative processes that can affect ERM. Review and revision processes should provide assurance that changes are evaluated, performance and risk are reviewed, and ERM remains effective. Review activities could include variance analysis, information comparisons, and tracking effectiveness and application of control activities. Review activities should be differentiated from activities already being performed as part of business processes. Reviews often take the form of self-assessments, where persons responsible for a unit or function determine the effectiveness of ERM for their areas of responsibility. The reviewer should understand the area of the institution or the ERM process being reviewed. Reviewers should document their work and can use tools such as checklists, questionnaires, flowcharting, or benchmarking for evaluations. If review processes identify concerns, management should complete revision processes, as needed. Evaluative questions and items to consider when examining review and revision processes include:

- ***Risk and Performance:*** **Do review activities provide reasonable assurance that risks are being managed within risk tolerances and are aligned with risk appetite? Are appropriate revisions made based on results from review activities?** Risk and performance reviews should be integrated into business practices and performed continually, as part of day-to-day discussions and decisions. The first line often conducts ongoing reviews, and the second line conducts quality control reviews. Some questions to consider during reviews include: are risk appetites and tolerances still appropriate; are all risks identified and assessed accurately; is performance on target; are the risk responses and control activities appropriate and being completed effectively; and is enough risk being taken to meet objectives? To the extent possible, any changes stemming from review activities should be based on the deviation level in performance, importance of the business objective, and the costs and benefits associated with a change. Changes stemming from review activities could include revisions to risk appetite, tolerances, responses, rating, or priority. Revisions may also include reallocating resources, revising business objectives, or exploring alternative strategies.

- ***ERM Processes:*** **Are review and revision activities conducted to identify and implement improvements to ERM processes?** ERM processes might not be conducted as efficiently or effectively as intended, causing risk to develop and impact performance. Even robust ERM programs can become more efficient through ongoing review and revision processes. By embedding continual evaluations into business practices, potential improvements to ERM can be identified and implemented. Opportunities to improve ERM processes include, but are not limited to, implementing new technology, revising risk criteria or categories, analyzing industry peers, enhancing communication, or making organizational changes (i.e., changes in governance structure).

Information, Communication, and Reporting: Management uses relevant information from both internal and external sources to support ERM. Communication is the continual process of obtaining information and sharing it throughout the institution. The institution leverages information systems to capture, process, and manage data and information. By using information obtained throughout the ERM process, the institution can report on risk and performance. Evaluative questions and items to consider when examining information, communication, and reporting include:

- ***Information:*** **Do information systems and the information obtained support ERM initiatives?** Complete and accurate information is necessary at all levels to identify, assess, and respond to risks, and to otherwise run the institution and achieve its objectives.

Appropriate information systems should be in place to manage and refine large volumes of data into actionable information. Data reliability and quality is critical with the increasing dependence on information systems and data-driven, automated decision systems. To ensure data quality, management should establish an enterprise-wide database management program. Refer to the *Operations* procedure in the *Information Technology & Security* Examination Manual topic for examining database management programs.

- ***Communication:*** **Are appropriate communication systems in place to deliver information to all levels of the institution, as necessary?** Communicating the appropriate information, on time and at the right place, is essential to effective ERM. For example, it is important that risk appetite and risk tolerances are communicated to staff. Information should be timely delivered to personnel in a form that enables them to carry out their role in ERM and other responsibilities. Communication systems and messaging processes can take many forms, such as electronic messages, external or third-party materials, informal and verbal communications, training and seminars, or written internal documents, such as reports, dashboards, policy, and procedures. The mode of communication should be appropriate for the message, and the tone should be consistent with the established risk culture.

- ***Reporting:*** **Is reporting effective in communicating the relevant aspects of ERM, any deficiencies, and elevated risks to the necessary parties?** An effective ERM program includes regular, meaningful reporting. Reporting becomes increasingly important as ERM matures, and the program is used to make business decisions. Reporting should provide assurance to the board and management that ERM processes are effective, support an understanding of risk and preparedness for risk events, and highlight changes in the risk profile. Reporting efforts should consolidate results into a meaningful format appropriate for the intended audience. Typically, high-level reports are completed quarterly or annually for the board, while reporting should be continuous at the operational level. ERM board reporting requirements should be outlined in board policy and should include additional expectations when risks change or are elevated beyond tolerances. Status reports should be provided to management and the board when risks exceed risk tolerance levels to determine if risk responses remain effective and actions taken to mitigate risks are appropriate. Additionally, changes in the risk universe (new or removed risks), risk ratings, or priorities, as well as proposed modifications to risk appetite, risk tolerances, business objectives, or strategies, should be reported to the board. Reports should include both quantitative and qualitative risk information. In addition to the reports outlined above, ERM reports could also include the following:

    - Institution-wide view of risk
    - Sensitivity analysis
    - Performance measures
    - Key performance indicators
    - Key risk indicators
    - Trend analysis
    - Results of review activities

Refer to the following for additional information and guidance on ERM:

- AICPA's 2017 The State of Risk Oversight: An Overview of Enterprise Risk Management Practices

- Office of the Comptroller of the Currency's handbook on Corporate and Risk Governance

2. Model Risk Management:

Evaluate the adequacy of processes and controls to govern the use of models.

Guidance:

System banks, associations, and service corporations (collectively *institutions*) often rely on models in many aspects of decision making. They routinely use models for a broad range of activities, such as valuing exposures, instruments, and positions; underwriting credits; measuring risk; developing financial plans; and determining capital and allowance for loss adequacy. As such, proper management of model risk is a crucial part of an institution's risk management framework. The following are key terms and considerations in the examination of model risk management (MRM):

- *Model Definition* – For purposes of this guidance, a model is defined as a quantitative methodology that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. Models use these methods to reflect estimates of real-world relationships between the input data and assumptions and the measured output. Considerations include:
    - A model as defined above consists of three components: 1) an information input component, which delivers data and assumptions to the model, 2) a processing component, which transforms inputs into estimates, and 3) a reporting component, which translates the estimates into useful business information.
    - A model with quantitative outputs may have inputs that are both quantitative and qualitative. Approaches that generate qualitative output are generally not defined as a model, but exceptions exist. For example, a loan underwriting model that converts quantitative information into qualitative output, such as an accept or reject decision, should be defined as a model. The assumptions and estimates used in this transformation are key considerations in determining if the approach is a model.
    - Worksheets and other end-user computer tools are models if they meet the above definition of a model. In addition, not all models involve complex mathematical techniques or require detailed computer programming code, but this does not diminish their potential importance and impact on decision-making.
    - In situations where the board and management are unclear about whether an application or tool is a model, they should be conservative and treat the application or tool as a model. Defining an application or tool as a model ensures it is captured in the MRM framework while still enabling the institution to differentiate its risk management processes based on model risk and materiality.
- *Model Risk* – Model risk is the potential for adverse consequences from decisions based on inaccurate or misused model inputs, outputs, and reports. The use of models invariably presents model risk, and can result in financial loss, poor business and strategic decision-making, or damage to an institution's reputation. This risk primarily occurs because the model may have fundamental input or design errors that produce inaccurate outputs. The risk may also occur from using the model incorrectly or inappropriately. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact.

- *Model Governance* – Similar to other risk exposures, model risk is managed by implementing strong governance practices. The board and senior management provide model governance by creating an overall MRM framework. This framework includes establishing policies and procedures, allocating resources, and assigning responsibilities and accountability. The board and management should also ensure independence in the audit process and create mechanisms for evaluating compliance with policies and procedures and the effectiveness of the MRM process.

- *Model Materiality* – Materiality is an important consideration in designing an MRM framework. Assessing materiality should be based on model risk and the potential impact of the institution's models on business decisions, financial performance, risk measurement and management, financial reporting, and reputation risk. If models or model outputs could have a material harmful impact, the MRM framework should be extensive and rigorous. If the use of models is not pervasive and has low impact, the MRM framework may be relatively simple. The proper assessment of model materiality is also an important consideration in differentiating MRM expectations for each model.

- *Effective Challenge* – Effective challenge is a guiding principle for managing model risk. Effective challenge refers to the critical analysis by objective, informed parties who can identify model weaknesses and limitations and produce appropriate changes. Effective challenge depends on a combination of incentives, competence, and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model owners and when challenge is supported by well-designed compensation practices and corporate culture. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique. Senior management is responsible for ensuring effective challenge.

The guidance below outlines baseline sound practices and recognizes that MRM processes may vary based on model materiality. This guidance is intended to be applied using a risk-based approach. Where models are significant, complex, and pose material risk, examiners should consider the additional standards described in the interagency guidance published by other financial regulators (Office of the Comptroller of the Currency Bulletin 2011-12, April 4, 2011; Federal Reserve Supervision and Regulation Letter SR 11-7, April 4, 2011; Federal Deposit Insurance Corporation Examination Policies Manual Section 4.1 on MRM and Financial Institution Letter FIL-22-2017, June 7, 2017). This guidance goes into more detail on MRM, including a comprehensive description of the various model validation processes.

Note: This examination procedure focuses on the overall MRM framework and not on individual models. Individual models are addressed in the applicable procedures throughout the Examination Manual. For example, we address the examination of interest rate risk model use and validation in the *Interest Rate Risk Management* Examination Manual topic. Examiners should consider the results from examining individual models when concluding on the effectiveness of MRM.

Evaluative questions and items to consider when examining MRM include:

- ***Policies and Procedures:*** **Do MRM policies and procedures provide adequate guidance and direction?** Policies or procedures should address all aspects of MRM, including model definitions; model risk assessments; model inventories; acceptable practices for new model development and implementation; model documentation; model validation; change controls and other controls over the MRM process; and reporting requirements. The board

should approve MRM policies and review them annually to ensure consistent practices across the organization commensurate with the materiality of model use. Procedures should contain sufficiently detailed information to ensure consistency and continuity of processes.

- ***Model Definition:*** **Does the institution accurately define a model?** Accurately defining a model is the first step in ensuring all models are captured in the MRM framework. Policies or procedures should document model definitions that are consistent with the definition provided earlier. Examples of models could include:

    - Allowance for loss analyses (including investment impairment)
    - Capital allocations
    - Economic capital
    - Credit scoring
    - Automated collateral evaluation
    - Economic projections
    - Loan pricing
    - Funds transfer pricing
    - Risk measurement
    - Financial planning and projections
    - Stress testing (e.g., credit, capital, earnings, liquidity, sensitivity, investments, and derivative stress testing)
    - Financial instrument valuation (e.g., applications for estimating or validating investment fair values)

- ***Model Inventory:*** **Does management maintain a model inventory that lists all models and includes relevant information on each?** Institutions should maintain a comprehensive inventory that lists models in use, under development, and recently retired. Such an inventory is an important internal control. It enables the institution to evaluate its aggregate model risk and ensure all models are addressed in the MRM framework and subject to the principle of effective challenge. The inventory should include all internally developed models, vendor models, and models shared with other System institutions. Generally, the inventory should address the following for each model:

    - Model risk and materiality
    - Model purpose
    - Business line responsible for the model (i.e., model owners)
    - Person or business unit responsible for the model's validation
    - Model validation status (including validation schedule)
    - Description of most recent major upgrade or model version

- ***New Model Development and Implementation:*** **Are processes for developing and implementing new models clearly defined and sound?** Model development and implementation includes all activities related to researching, developing, documenting, testing, and deploying both internally-developed and vendor-developed models. As noted above, MRM policies and procedures should provide clear standards for model development and implementation. The following are key considerations:

    - The model development process should start with a clear statement of purpose that ensures the model is aligned with its intended use. The design, theory, and logic underlying the model should be well documented and aligned with published research and sound industry practice. Developers should ensure the components

work as intended, are appropriate for the intended business purpose, are adequately supported by the information technology infrastructure, and are conceptually sound and mathematically and statistically correct.

- Model development should include a data quality and relevance assessment and appropriate documentation to demonstrate that such data and information are suitable. If data and information are not representative of what they are intended to capture, or if assumptions are needed to adjust the data and information, these factors should be properly identified, analyzed, and documented. This is important so that users will be aware of potential limitations.

- The model should be rigorously tested under various assumptions, including assumptions and scenarios outside the range of ordinary expectations, to ensure it will perform as intended. Any deficiencies identified during testing should be corrected prior to a model being used in production. A model under development should not be used for conducting business activities.

- Model testing should assess inherent model inaccuracy and uncertainty. These assessments should be quantified if possible, such as by measuring the potential impact of factors that are not observable or incorporated into the model. At times, only a qualitative assessment may be possible. To account for model inaccuracy, it can be prudent to report a range of outcomes or apply judgmental conservatism to assumptions and model output. However, such conservatism should not impede proper model development and application or be used as a solution that dissuades the institution from improving the model.

- Third-party vendor models pose unique challenges for MRM, particularly when some model components are considered proprietary, and users cannot access computer code or mathematical formulas. Nonetheless, vendor products should be incorporated into the institution's model development and implementation standards following the same principles as applied to in-house models, although the process may be modified. While vendor products may provide a means of outsourcing model development, it is important to understand that model risk itself is not outsourced and is still held by the institution. Customization of the vendor model, including model settings, should be documented and tested to ensure the model will function as intended. The model's ability to reasonably capture the institution's unique risks or positions should be thoroughly assessed. Model documentation should be commensurate with expectations for an internally developed model of similar model risk and materiality. The vendor should be expected to:

    - Provide information on model components, design, and intended use to determine whether it is appropriate for the institution.

    - Identify the model's limitations, assumptions, and any areas where model use may be problematic.

    - Provide evidence that their product works as expected.

    - Provide ongoing support with appropriate model updates, as needed, including a description of the changes and potential impact on results.

- ***Model Validation:*** **Do effective processes exist to periodically validate models consistent with their risk and materiality?** After new models are tested and implemented, processes should be established to validate the models. Model validation plays a critical role in MRM and should be consistent with the principle of effective challenge. Validation involves processes and activities intended to verify models are performing as expected and are in line with their design objectives and business uses. Effective validation helps ensure models are sound. It also identifies potential limitations of the model and assumptions and assesses their possible impact. All model components, including input, processing, and reporting, should be subject to validation. This applies equally to models developed in-house and to those developed by third-party vendors. Institutions need to validate their own use of vendor models. As previously discussed, the model validation process should be addressed in the MRM policies or procedures. Additional considerations include:
    - Validation should include ongoing performance monitoring and periodic comprehensive activities. Ongoing performance monitoring is important to minimize the time lag in identifying deficiencies in regularly used models. Periodic validation is important to comprehensively evaluate the continued conceptual soundness of the model. Examples of validation activities include:
        - Comparing model outputs to actual outcomes, including causes and quantified attribution of differences.
        - Validating changes to the model (a component of change controls).
        - Evaluating required model overrides.
        - Evaluating whether changes in products, exposures, activities, market conditions, or management processes (e.g., underwriting standards) necessitate changes to the model.
        - Analyzing model sensitivity to key inputs and assumptions.
        - Benchmarking model results.
        - Backtesting model results.
        - Analyzing whether model use remains aligned with the intended purpose and has not been broadened beyond the model's capability (model risk significantly increases if models are used incorrectly or inappropriately).
        - Validating that data input, assumptions, and model design remain appropriate and representative of what is being measured and consistent with sound industry practices.
    - The frequency and scope of validation should be commensurate with the complexity, materiality, and potential impact of the model. Models should be reviewed at least annually to determine if the existing validation plans and activities are sufficient. Such a determination could simply affirm previous validation work, suggest updates to previous validation activities, or call for additional validation activities. It is a sound practice to ensure that all material models undergo a

comprehensive validation at some fixed interval, including updated documentation of all activities.

- Validation activities require a degree of independence from model development and use. Generally, parties not responsible for development or use and without a stake in a model's validity should complete the validation activities. However, as a practical matter, model developers and users may be the most effective in completing some of the validation work. In such cases, it is essential that their validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. The board and management may need to periodically engage external resources to obtain the necessary specialized expertise and independence for model validation.

- ***Change Controls:*** **Do sufficient controls exist to manage changes to models?** Controls should limit access to model programming, settings, data input, and assumptions. Controls should also ensure significant changes to models are validated, approved, and reported under established authorities. The board and management should delegate authority based on materiality and impact of the model change. Each model should have a change control log that states when the model was changed, the nature of the change, who was responsible for the change, and who approved the change. The change control log allows others to clearly understand changes to a model's functions and settings, and aids in its auditing. Change controls should be commensurate with model complexity, risk, and materiality. Policies or procedures should address change control processes.

- ***Internal Controls:*** **Do sufficient internal controls exist over MRM processes?** In addition to the controls described previously, effective internal controls should include adequate staffing, enforcement of delegated authorities, separation of duties, and a qualified, independent audit. More specifically:

  - *Staffing* – The board and management should allocate sufficient staffing resources to MRM commensurate with model risk and materiality. Staff involved in model development and use, validation, and audit should have the requisite knowledge, skills, and expertise. Where necessary skills are difficult to hire or retain, the institution may co-source some activities, such as the independent model review and validation.

  - *Delegations of Authority* – The board and management should clearly define and formally document staff roles, responsibilities, and authorities for each key facet of the MRM framework.

  - *Separation of Duties* – MRM is more effective when there is a greater separation between those who challenge models (e.g., model validation, as discussed previously) and those that develop and use models. If full separation is not practical, mitigating internal controls should be established.

  - *Audit* – A qualified internal auditor or outside independent party should periodically review the MRM framework and processes for adequacy, including compliance with MRM policies and procedures. Internal audit should be independent of MRM functions. If internal audit staff perform validation activities, the audit staff member(s) involved in the validation should not be involved in audit work related to

those models or the overall MRM framework assessment. Refer to the *Audit* procedure for examining audit coverage.

- ***Board Reporting:*** **Is reporting timely, accurate, and sufficient for the board to monitor model risk and make informed MRM decisions?** Board reporting should occur at least annually and comply with the reporting requirements in policies. Reporting should be commensurate with model risk and materiality and, at a minimum, address model inventories, significant model changes, model validation activities, and results from any internal and external audits and reviews of MRM (including management responses and resolution of recommendations).

- ***Results from Examination of Individual Models:*** **Did our examination of individual models evidence effective implementation of MRM policies, procedures, and practices, including effective model validation activities?** Conclusions on MRM should consider results from the examination of individual models. Individual models are addressed in the applicable procedures throughout the Examination Manual.

3. Third-Party Risk Management:

Evaluate the adequacy of processes and controls to govern third-party relationships.

Guidance:

Competition, advances in technology, and innovation within the financial services industry have prompted institutions to actively seek ways to reduce costs, obtain expertise, expand customer product offerings, and improve services. As a result, it is common for institutions to outsource with third-party vendors or service providers for products, processes, systems, and services that might otherwise be developed or completed in-house. Some examples are information technology, audit, appraisal, human resources, and legal services. Outsourcing, however, does not change the expectation to operate in a safe and sound manner. Risk exists whether the institution develops and maintains the products, processes, systems, and services internally or outsources them. When relying on outsourcing, the board and management are responsible for understanding the risks and ensuring effective third-party risk management practices. As part of sound risk management, institutions should engage in more comprehensive and rigorous oversight and management of third-party relationships that support critical activities. Critical activities include products, processes, systems, or services that could have a significant impact on the institution and its customers if the third party does not perform as expected.

When applying the sound business practice criteria in the evaluative questions below, examiners should consider the extent, complexity, and risk of the institution's outsourcing to third parties. As these factors increase, institutions should have a more formalized (i.e., defined, comprehensive, and documented) third-party risk management program. Refer to FCA's Informational Memorandum on Risk Management of Outsourcing dated October 25, 2000, for information and guidance on the areas discussed below. The Interagency Guidance on Third-Party Relationships: Risk Management dated June 6, 2023 and Third-Party Risk Management: A Guide for Community Banks dated May 2024 from other financial regulators provides complementary and additional guidance about managing risk in third-party relationships. In addition, refer to the Federal Financial Institutions Examination Council booklet on Outsourcing Technology Services.

Note: This examination procedure focuses on the overall processes and controls for managing third-party risk and relationships rather than examining individual relationships with specific vendors or

service providers. Individual third-party relationships are examined using the applicable procedures throughout the Examination Manual. For example, we address the examination of outsourced audit and review resources in the *Audit & Review Programs* Examination Manual topic. Examiners should consider the results from examining individual third-party relationships when concluding on the effectiveness of third-party risk management.

Governance: The board is accountable for overseeing outsourcing and third-party relationship programs, while management is responsible for developing and implementing appropriate processes and controls to manage these relationships. Evaluative questions and items to consider when examining third-party risk governance include:

- ***Strategic Direction:*** **Does the board and management ensure outsourcing decisions are consistent with strategic plans?** The board and management should ensure that critical outsourcing decisions are consistent with the institution's short- and long-term goals and strategic plans. Management should periodically report to the board to demonstrate this. Processes should be in place to evaluate potential and existing third-party relationships to determine how they fit with strategic plans. Examples of items to consider for critical third-party relationships, as defined by the institution, include:

    - Purpose of outsourcing and how it aligns with strategic goals, policies, and risk appetite.
    - Cost-benefit of outsourcing.
    - Impact on employees and customers.
    - Complexity of the product, process, system, or service being outsourced.
    - Monitoring and oversight requirements.
    - Information security implications.
    - Regulatory implications.
    - Other key risks associated with outsourcing the product, process, system, or service.
    - Contingency considerations for when outsourcing needs change, an existing contract expires, or a third party is no longer fulfilling contract terms.

- ***Policies and Procedures:*** **Do third-party risk management policies and procedures provide adequate guidance and direction?** FCA Regulation 609.930(c)(5) requires the board to develop policies for vendor management and oversight. Board policies should provide sufficient guidance to govern outsourcing processes and expectations. The board needs to periodically review and approve these policies to ensure they reflect any changes in the risk environment and the board's expectations. Procedures should align with related policy guidance and provide sufficient direction to staff on the primary processes and controls related to third-party risk management. Institutions may include related guidance in its Enterprise Risk Management framework. The following are examples of items that should be addressed in policies or procedures based on the extent, complexity, and risk of outsourcing to third parties:

    - Risk appetite for using third-party relationships.

    - Guidance for making outsourcing decisions, selecting vendors or service providers, and negotiating contracts, including criteria for requiring board approval of critical relationships and contracts.

    - Expectations for maintaining a third-party relationship inventory.

- Methodology for completing the required risk assessments of relationships with all vendors or third parties, including the use of risk criteria and risk ratings.
- Processes for monitoring, changing, and discontinuing (or terminating) relationships, including contingency planning.
- Responsibilities and accountability for monitoring and managing relationships.
- Requirements for reporting, including criteria for escalating issues to the board and management.

Inventory and Risk Assessment: Management should inventory third-party relationships and assess the risks of outsourcing products, processes, systems, or services. The inventory and risk assessment should be reviewed annually and updated as needed. Evaluative questions and items to consider when examining third-party inventories and risk assessments include:

- ***Inventory:*** **Does management maintain an accurate inventory of its third-party relationships?** Before assessing the risks associated with third-party relationships, an inventory of those relationships is needed. In addition to identifying the name of the third party, the inventory should include information such as a description of the product, process, system, or service being provided, and identification of who is responsible for monitoring and managing the relationship. Inventories might also identify the types of data or information (i.e., public, confidential, sensitive) the third party would be able to access. Some of the more common relationships may include, but are not limited to:
  - Other System institutions, service corporations, affiliates, and joint ventures.
  - Professional services such as attorneys, appraisers, auditors, consultants, and tax preparers.
  - Software and hardware providers.
  - Entities that support human resource functions such as payroll or benefits.
  - Financial market utilities such as clearing houses, wire transfer services, and credit card providers.
- ***Risk Assessment:*** **Does management have an effective process to periodically assess and document the risks in third-party relationships*?*** FCA Regulation 609.930(c)(5)(iii) requires the institution to conduct a vendor risk assessment on all vendors, including non-IT vendors. The risk assessment process should follow a defined methodology for risk rating each relationship identified in the third-party inventory (e.g., low, moderate, or high risk). Not all third-party relationships present the same level of risk and use of third parties may introduce new risks or increase existing risks. Management should establish criteria for assessing risk in third-party relationships and apply it consistently to each relationship. The criteria should sufficiently consider areas such as operational, compliance, reputation, strategic, and credit risk, and risk mitigation. Criteria should also include both quantitative and qualitative factors and consider both inherent and residual risks. Risk assessments should also consider risk associated with reliance on a single vendor and vendors located in the same geographic area (especially those prone to natural disasters). The individuals responsible for managing and monitoring these relationships should provide input into the risk assessment. The resulting risk ratings help determine the level of due diligence and monitoring needed, as well as identify overall third-party risk across the institution. This process should also identify any concentrations of risk among different relationships. Banks

should consider concentration risks when multiple institutions across the System or within a district use the same third party to ensure such risks are sufficiently identified and addressed.

Selection and Contracts: It is important that institutions conduct sufficient due diligence before selecting and entering relationships with third-party vendors or service providers. Additionally, management should ensure formal contracts with appropriate provisions are used, as applicable. Evaluative questions and items to consider when examining processes for selecting and establishing contracts with third parties include:

- ***Selection:*** **Are sufficient processes in place to perform and document the due diligence necessary to select third-party vendors or service providers?** FCA Regulation 609.930(c)(5)(i) requires the institution to exercise appropriate due diligence in selecting vendors. Due diligence for third-party vendor or service provider selection involves a technical, functional, and financial review to identify potential risks and verify the third party's ability to deliver the proposed requirements. Those assigned to conduct due diligence reviews should possess the requisite expertise to understand the product, process, system, or service being outsourced and the institution's needs. Depending on what is being outsourced and the level of in-house expertise, the institution may also consider the assistance of a consultant familiar with outsourcing arrangements who can help determine the scope of services needed and evaluate the qualifications of the prospective third party. The level of due diligence and related documentation should be commensurate with the level of risk the third-party relationship presents. The intent is to verify and assess information about the third party, such as:
    - Business experience, qualifications, and reputation.
    - Business strategies and goals.
    - Legal and regulatory compliance, including necessary licenses.
    - Financial condition and stability.
    - Risk management program and internal control environment, including internal and external audit functions, service organization control reports, and fraud prevention processes.
    - Information security program, physical security controls, management of information systems and subcontractors, and business continuity and disaster recovery plans and processes, as applicable.
    - Insurance coverage (e.g., fidelity bond, liability, and hazard).
    - Human resource management (e.g., succession planning, performance management, and training).
    - Reliance and management of subcontractors.
- ***Contracts:*** **Are processes in place to ensure contracts, when necessary, are used effectively to govern third-party relationships?** FCA Regulation 609.930(c)(5)(ii) requires the institution to negotiate contract provisions that facilitate effective risk management and oversight and specify the expectations and obligations of both parties. A written contract is one of the

most important risk management controls in the outsourcing process. Contracts should clearly define the rights and responsibilities of the third party and the institution. Properly documenting this information protects the institution's interests, minimizes misunderstandings between the parties, and helps ensure the ongoing service provided is consistent with the board and management's expectations. Management should ensure effective processes and controls are in place on using contracts, including involving legal counsel early in the process to help prepare and review proposed contracts, particularly those involving critical activities. When required by policy, management should obtain board approval of contracts. To help evaluate the use of contracts, examiners could sample third-party relationships to determine the effectiveness of contracts for those relationships. Examples of items that should be considered (as applicable) when negotiating contracts include:

- Scope of service
- Performance standards (service level agreements or minimum requirements), including ethical conduct
- Security and confidentiality, especially of sensitive data
- Audit and remediation requirements
- Reporting requirements
- Business resumption and contingency plans
- Subcontracting
- Notification requirements (disaster recovery, non-compliance, data breach)
- Cost and compensation
- Ownership and licensing (data, hardware, software, and intellectual property)
- Duration (contract length and renewal periods)
- Insurance requirements
- Dispute resolution
- Indemnification
- Limitation of liability
- Default and termination
- Assignment
- Regulatory compliance and FCA enforcement authority

Monitoring, Reporting, and Other Controls: Management should implement a program to monitor and manage third-party risk and performance with periodic reporting to the board. The board and management should use the results of ongoing monitoring activities and reports when updating risk assessments and making strategic decisions associated with outsourcing. Not all relationships present the same level of risk and therefore do not require the same level of oversight and risk management. Evaluative questions and items to consider when examining third-party risk management monitoring, reporting, and other controls include:

- ***Monitoring:*** **Does management maintain an effective program to monitor third-party relationships and risks?** Monitoring processes should ensure third-party vendors and service providers deliver the quantity and quality of products and services required by the contract. Ongoing monitoring with appropriate documentation is important for contract negotiations, termination issues, and contingency planning. The resources devoted to monitoring activities will depend partly on the risk and complexity of the products, processes, systems, or services outsourced. Management should assign responsibility for monitoring and managing third-party relationships to specific personnel or a committee. These individuals should have the expertise and authority to oversee and monitor the relationship. Lower-risk

relationships may require limited monitoring, while critical relationships would require more extensive monitoring, including periodic visits or meetings with third-party representatives. Monitoring should typically include performing and documenting periodic reviews of the third-party's financial condition, audit and internal control reports, and changes to operations. More specifically, these reviews should include the same areas considered during due diligence when selecting third parties. The institution should use information obtained during monitoring to ensure third-party vendors and service providers are meeting contractual obligations and to update the third-party risk assessment, if warranted. To help evaluate monitoring processes, examiners could sample third-party relationships to determine the effectiveness of monitoring activities.

- ***Reporting:*** **Is reporting timely, accurate, and sufficient for the board and management to oversee third-party risk management and make informed outsourcing decisions?** Reporting should be commensurate with the criticality and significance of the institution's outsourcing activities. Individuals responsible for oversight should escalate significant issues identified during monitoring to management and the board in accordance with established reporting expectations. Board reporting should occur at least annually and comply with the reporting requirements in policies. Board minutes and related materials should evidence reporting on board approvals required by policy, monitoring activity results, due diligence summaries, and other key information to assist the board in its oversight of third-party risk management.

- ***Internal Audit:*** **Is third-party risk management appropriately considered in the audit universe and audited periodically?** Third-party risk management should be considered for audit periodically based on risk assessed, similar to other auditable areas. Refer to the *Audit* procedure for examining third-party risk management audits.

- ***Results from Examination of Individual Third-Party Relationships:*** **Did our examination of individual third-party relationships evidence effective implementation of third-party risk management policies, procedures, and processes?** Conclusions on the adequacy of third-party risk management should consider results from the examination of individual third-party relationships in the applicable procedures throughout the Examination Manual.

4. Stress Testing Framework:

Evaluate the adequacy of processes and controls to govern the stress testing framework and related activities.

Guidance:

Stress testing is a critical risk management tool for System institutions. We expect all System institutions to have a stress testing framework consistent with the principles outlined in FCA's Informational Memorandum on Stress Testing Expectations dated September 8, 2023. The framework (i.e., policies, procedures, processes, and controls) will vary based on the size, complexity, and risk profile of the institution. Establishing an appropriate framework encompassing the core principles outlined in the informational memorandum helps ensure stress testing activities result in relevant information that can be used in risk management and strategic planning processes. The Interagency Guidance on Stress Testing dated May 14, 2012, contains additional information on stress testing frameworks.

An effective stress testing framework covers the institution's full set of material exposures,

activities, and risks based on effective enterprise-wide risk identification and assessment. The framework should cover stress testing activities applied at various levels in the institution (e.g., business line, portfolio, risk type, enterprise-wide basis). The framework should employ multiple conceptually sound stress testing activities and approaches. It should also be forward-looking and flexible with clear, actionable, well supported results to inform decision making. A well-structured and supported framework provides key information into the potential adverse outcomes arising from a wide range of risks, making it an important component of managing risk within the board's risk appetite. The framework should define the role of stress testing as part of the institution's key risk management practices. Moreover, the framework should establish the expected depth and breadth of the institution's stress testing work, ensuring each activity is commensurate with the institution's size, complexity, and risks.

The concepts outlined in this procedure should be applied to all stress testing activities conducted within the institution, including, but not limited to, stress testing activities covered in the following Examination Manual topics:

- *Capital Management*
- *Investments*
- *Portfolio Planning & Analysis*
- *Collateral Risk Management*
- *Earnings Management*
- *Liquidity Management*
- *Interest Rate Risk Management*
- *Derivatives*

While many stress testing activities are specific in scope and focus, examiners should consider the interrelationships among the specific risks evaluated. A sound stress testing framework allows for an enterprise-wide view of risk, including the aggregation of related risk impacts where appropriate.

Note: This procedure examines the overall framework for governance of stress testing activities at the institution. Examinations of specific stress testing activities should be completed under the applicable topic in the Examination Manual. For service corporations, this guidance should be considered in the context of their specific role in stress testing activities.

Evaluative questions and items to consider when examining the stress testing framework include:

- ***Governance:*** **Is there a well-defined governance structure in place for the stress testing framework and related activities?** A sound stress testing framework includes governance structures that promote comprehensive and consistent oversight and monitoring of stress testing activities and maintains independence and objectivity. Though the board has the ultimate responsibility, the board and management are responsible for developing a sound stress testing framework, establishing stress testing objectives, and carrying out meaningful and actionable stress testing activities commensurate with the size, complexity, and risk profile of the institution. The institution may also establish a stress-testing committee or similar body responsible for overseeing the stress testing framework and related activities. Policies, procedures, or committee charters should outline the governance structure. The framework should ensure stress testing activities are not isolated within a specific operational function, but are firmly integrated into the risk management practices of business lines, capital and financial planning, asset-liability management, and other decision-making processes. Processes should encourage collaboration between stakeholders and foster effective challenge at each key stage of the stress testing process. This includes

scenario development and approval, model development and validation, data sufficiency and limitations, reporting, and the use of stress test results. Lastly, mechanisms should be in place to address any identified deficiencies or weaknesses in the stress testing framework, including a process for remediation and continuous improvement.

- ***Policies and Procedures*: Do stress testing policies and procedures adequately define the stress testing framework and provide adequate direction and guidance for related activities?** Policies and procedures should outline the stress testing framework governance structure and the objectives, scope, frequency, and reporting requirements of all stress testing activities. Consistent with FCA's Informational Memorandum on Stress Testing Expectations dated September 8, 2023, board policy should communicate the objectives of the stress testing framework and expectations for how stress testing results are reported and used in decision-making processes (e.g., capital and business planning, risk management, and other processes). Policies and procedures should ensure effective communication to all relevant stakeholders, including the board, senior management, risk committees, and external parties as applicable. Policies and procedures should also specify clear roles for the board, senior management, and other staff as discussed in the *Roles and Responsibilities section* below. Additionally, policies and procedures should be regularly reviewed and updated to reflect changes in risk profile and other operational changes. Procedures should ensure stress testing activities and processes are consistent with policy direction and support the stress testing framework's objectives and the institution's risk management initiatives. Procedures should address all key aspects of the stress testing framework and related processes, including, but not limited to the following:

    - Identifying relevant risks.
    - Developing, documenting, and reviewing stress testing processes, scenarios, and key assumptions.
    - Reviewing, challenging, and reporting results.
    - Assessing the ongoing performance and effectiveness of the stress testing framework and related activities.

- ***Roles and Responsibilities:* Have roles and responsibilities for key stress testing stakeholders been clearly documented?** An effective stress testing framework requires robust involvement from all stakeholders. The framework should identify all key internal and external stakeholders (e.g., stockholders, FCA, funding bank, institution staff, audit) with key roles documented. The board and management should allocate sufficient resources, such as funding and staffing to the institution's stress testing framework and related activities. Staffing for stress testing activities should be commensurate with the institution's needs. Policies, procedures, charters, and job descriptions should specify the roles and responsibilities of all key stress testing stakeholders. Roles and responsibilities should be established not only for the board and senior management, but also for technical experts, business unit managers, risk managers, and internal auditors. Processes should be in place to facilitate communication and collaboration between stakeholders. While actual assignments and duties may vary, the following outlines common responsibilities and roles in a stress testing framework:

    - *The Board* – The board has ultimate responsibility for establishing objectives and setting expectations for the stress testing framework and related activities. The board should approve policy and relevant committee charters, review and challenge stress test results, and provide feedback. Board members should also have the

opportunity to provide high-level, front-end input into the stress testing framework and related activities by identifying risks, assets, portfolio segments, or economic factors of particular interest or potential concern (e.g., a new lending program, substantially increased lending efforts in one specific area, changing interest rate risk management strategies). The board should actively review and discuss stress testing reports (both individual and enterprise wide), evaluating results relative to

risk appetite, overall strategy and business plans, and contingency plans. If results are inconsistent with objectives in these areas, the board should direct change.

- *Senior Management* – Senior management is responsible for incorporating stress testing activities into the risk management practices of the institution, consistent with the board's objectives. Senior management should oversee stress testing efforts, formulate conclusions, and develop risk management strategies, responses, and recommendations based on stress test results. It is a sound practice for senior management to review stress testing activities regularly to evaluate and challenge, among other things, the validity of the assumptions, the severity of tests, the robustness of the estimates, the performance of underlying models, and the stability and reasonableness of the results. Senior management, directly and through relevant committees, is typically responsible for regular reporting to the board on stress testing developments and results and compliance with stress testing policy.

- *Staff* – Staff conduct stress testing activities in accordance with the stress testing framework and related policies and procedures. This includes completing the stress testing activities and ensuring the scenario(s), assumptions, risk factors, data, modeling, and reporting have the proper inputs and controls. Staff may be tasked with assisting senior management with developing scenarios, running the stress testing models, analyzing results, and drafting reports to communicate the results of the stress testing activities. Staff should possess the experience and specialized skills necessary to carry out stress testing activities that align with the complexity of institution operations or portfolios. Staff should have the proper training to ensure understanding of and adherence to not only the institution's stress testing framework but also applicable model risk management requirements, internal controls, and other related internal requirements. As the institution's risk profile and complexity increase, staffing levels and experience should also increase (which could include using external parties). Refer to FCA's Informational Memorandum on Stress Testing Expectations dated September 8, 2023, for additional guidance on stress testing resources.

- ***Other Internal Controls:*** **Do sufficient internal controls exist over the stress testing framework?** In addition to the controls described previously, effective internal controls should address documentation standards, data and models, and an independent audit as described below:

  - *Documentation Standards* – The board and management should set expectations around documentation requirements for assumptions, uncertainties, and limitations of stress testing activities. All stress tests, including well-developed quantitative tests supported by high-quality data, use a certain amount of expert or business judgment, and the role and impact of such judgment should be clearly documented.

  - *Data and Models* –Controls should be in place to aid in accurate and reliable data

used in stress testing and the stress testing framework should align with the model risk management framework. The institution should have the data and information technology infrastructure to perform stress testing effectively. The institution should have controls and processes in place to provide reasonable assurance over the adequacy, reliability, and timeliness of data used in stress testing activities. It should also have information systems capable of retrieving, processing, and reporting the information needed to support stress testing activities. Additionally, all stress testing models should be subject to sound governance under the institution's model risk management framework as discussed in the *Model Risk Management* procedure.

- *Audit* – Stress testing should be included in the audit universe and considered for periodic audits based on risk assessed, similar to other auditable areas. A qualified internal auditor or outside independent party should periodically review the stress testing framework and processes for adequacy, including compliance with applicable policies and procedures. Internal audit should be independent of stress testing functions. If internal audit staff perform validation activities, the audit staff member(s) involved in the validation should not be involved in audit work related to those models or the overall stress testing framework assessment. Refer to the *Audit* procedure for examining stress testing framework audits.

- ***Results from Examination of Individual Stress Testing Activities:*** **Did our examination of individual stress testing activities evidence effective implementation of the stress testing framework (policies, procedures, processes, and controls)?** Conclusions on the overall stress testing framework should consider results from the examination of individual stress testing activities. For example, if weaknesses were identified in an examination of a specific stress testing activity, the cause for the weakness may be in the overall stress testing framework. Individual stress testing activities are addressed in the applicable procedures throughout the Examination Manual.

5. Cooperative Principles:

Evaluate efforts to uphold a cooperative business culture and involve customers in the governance of the institution.

Guidance:

The Farm Credit System (System), as explained in Section 1.1 of the Farm Credit Act of 1971, as amended (the Act), is cooperatively structured "to accomplish the objective of improving the income and well-being of American farmers and ranchers by furnishing sound, adequate, and constructive credit…" Every System institution chartered by FCA is a member of the System under Section 1.2 of the Act. As such, all chartered institutions are bound to uphold the System's cooperative business culture.

A cooperative structure is one where members own and control their institution and receive benefits from doing business with it. Congress set up this ownership structure to keep the System committed to servicing agricultural and rural credit needs under the theory that having the borrowers participate in the operations of the institution will prevent System institutions from acting solely as private money-making organizations.

The generally accepted standards for cooperatives were established in 1844 and are known as the Rochdale Principles. The System is guided by these general cooperative principles, which can be summarized into the following three core principles as the foundation for the System's structure:

- *Member ownership* – This occurs through the purchase of voting stock with equitable voting rights.
- *Member control* – This is visible in the board composition, election activities, and annual meetings.
- *Member benefit* – This occurs through access to quality and affordable credit and related services and the payment of patronage. Young, beginning, and small farmers and ranchers are System beneficiaries in that they can receive credit services that may not otherwise be available to them. Other examples of the benefits of System institution membership include, but are not limited to, pooled risks, shared equity, lower cost of funds, and borrower rights.

Cooperatives are, by definition, entities with a member focus. Cooperative entities that focus on serving and fulfilling the needs of their members often realize greater participation in the cooperative by those members. System institutions should strive to achieve reputations as effective cooperatives and continually build on their efforts by maintaining a strong cooperative business culture.

In addition to specific regulations and the guidance documents referenced below, FCA's Informational Memorandum (IM) on Serving the Members of Farm Credit System Institutions dated November 4, 2010, serves as criteria for this examination guidance. This IM reinforces FCA Board Policy Statement 80 by encouraging boards and management to operate in a cooperative manner by engaging, communicating with, and providing value-added benefits to all members. FCA also provides guidance for directors in The Director's Role, which discusses cooperative principles and how institutions should ensure they are applied.

Evaluative questions and items to consider when examining the institution's implementation of cooperative principles include:

- ***Regulatory Compliance:*** **Does the institution comply with FCA Regulations on implementation of cooperative principles?** FCA Regulations 611.350 and 615.5230 identify specific requirements on voting practices and equitable treatment that directly relate to cooperative principles. Additionally, FCA Regulation 618.8440(b)(8) requires institutions to have a marketing plan that addresses how they will be responsive to the credit needs of all types of agricultural producers having a basis for credit, as set forth in Section 1.1(b) of the Act. Refer to the *Director Elections* procedure in the *Director Elections & Qualifications* Examination Manual topic, the *Capital Distribution Programs* and *Capital Compliance* procedures (and related workpapers) in the *Capital Management* topic, and the *Constructive Credit & Services* procedure in the *Mission Compliance* topic for guidance on examining compliance with these regulations. Examiners should consider the results from these procedures when concluding on an institution's effectiveness in implementing cooperative principles.
- ***Member Engagement:*** **Do the board and management effectively engage members as owners?** Engagement requires member-borrowers to be informed about their ownership rights, benefits, and participation opportunities in their institution. Examples for engaging members include:

- Providing complete and transparent disclosures at loan origination, in periodic financial reports, and in other communications.
- Informing members on how they can bring matters to the attention of the board or whole membership. This includes ensuring shareholder petition rights are understood, supported, fair, and reasonable.
- Maintaining an effective director election process that informs members of opportunities to serve as a director or on the Nominating Committee.
- Facilitating stockholder-to-stockholder communication by providing stockholder lists when requested (in accordance with FCA Regulation 618.8310).
- Promoting active member participation in shareholder meetings by:
  - Implementing various opportunities for meeting attendance, including in person and technological options. Institutions that use online meeting space as part of a meeting or election must have policies and procedures that address the requirements in FCA Regulation 611.110(c).
  - Polling members for their concerns or suggested agenda items.
  - Encouraging open discussion at meetings.
  - Holding a series of meetings at different locations.
  - Subsequently informing the membership of the level of attendance and actions taken at meetings.

- ***Member Communications:*** **Do the board and management communicate effectively with members?** Directors have a fiduciary duty to maintain open and direct communication with members, so that member interests are thoroughly considered and adequately represented. Institutions should provide members numerous opportunities to communicate and interact with directors and management. Examples of how to communicate with members include:
  - Employing ongoing, two-way communication with member-borrowers at regular stockholder meetings or by using tools such as comment cards, online suggestion portals, advisory stockholder committees, customer appreciation meetings, etc.
  - Routinely communicating the institution's mission, purpose, and cooperative philosophy. This can be through various documents including the business plan, bylaws, membership memos, annual meetings, stockholder reports, or other relevant documents.
  - Using both traditional methods and technology to share important information, including bylaws, notifications of stockholder action, and stockholder reports, as well as information on member benefits and services offered. Note: Institutions that use technology for communication must have policies and procedures that address the requirements in FCA Regulations at Part 609.

- Using flexible approaches to facilitate communication and involvement across large territories, such as webinars, conference calls, local informational sessions, and focus group meetings.

- ***Member Benefit:*** **Do the board and management provide value-added benefits to members?** Benefits should be designed to help members remain successful and encourage their interest in the institution. Member benefits should be routinely communicated to stockholders and the community. Examples of how to provide value-added benefits to members include:

  - Returning profit generated by the institution to members through patronage distributions while balancing the institution's capital needs.

  - Maintaining a compliant borrower rights program and a culture that puts members first.

  - Providing related services based on the needs of members, such as estate planning, recordkeeping, tax planning and preparation, crop insurance, credit life insurance, and farm business consulting. (Note: See the approved related services list on the FCA website.)

  - Upholding a commitment to young, beginning, and small farmers and ranchers by actively promoting credit opportunities or providing education, training, or special programs.

  - Providing outreach, education, training, and information to all eligible borrowers and the communities in which they live and work.

  - Exploring different financing structures to meet the needs of borrowers and those credit terms best suited for all types of agriculture practiced in the community.

- ***Wholesale Funding Arrangements (Banks Only):*** **Do bank policies and procedures adequately define the objectives of the district's wholesale funding arrangements and provide an adequate framework to guide related board and management decisions?** FCA Bookletter BL-074 describes how various interrelated processes are used to support cooperative principles and the cooperative operating philosophies outlined in FCA Board Policy Statement 80. Policies and procedures should provide for a mechanism to ensure bank processes are achieving the board's wholesale funding objectives. The banks use several interrelated processes to achieve these objectives which may include the following:

  - Wholesale credit policies (as required under FCA Regulation 614.4120)
  - Wholesale loan pricing or interest rate plans
  - Asset-liability management
  - Liquidity risk management
  - Enterprise risk management
  - Strategic and operational planning
  - Patronage
  - Funds transfer pricing

6. Bylaw Administration:

Determine if processes for maintaining and implementing bylaws are adequate and comply with regulatory guidance.

Guidance:

Bylaws are a set of rules that specify how the institution will operate within its corporate charter and framework. Institutions should review and update bylaws periodically, as needed, to address changes in regulatory requirements, the operating environment, or the institution's desired business practices. The board can typically make most bylaw changes, although some can require stockholder approval. To ensure bylaws remain current and relevant, the institution should have effective bylaw administration processes.

Note: This examination procedure focuses on bylaw administration and not on individual bylaws. Individual bylaws are addressed in the applicable Examination Manual procedures. For example, we address the examination of capital bylaws in the *Capital Management* Examination Manual topic. Examiners should consider the results from examining individual bylaws when concluding on the effectiveness of bylaw administration. As a reminder, FCA is prohibited under Section 5.17(b) of the Farm Credit Act of 1971, as amended from directly or indirectly approving bylaws. FCA examines for bylaw compliance with laws and regulations.

Evaluative questions and items to consider when examining bylaw administration include:

- ***Board Involvement:*** **Is the board sufficiently involved in bylaw administration?** The board needs to be involved in the review, revision, and approval of bylaws. While management may draft bylaw revisions, the board needs to provide direction on the revisions and ensure it understands them. Management typically provides the board a redline copy of proposed bylaw revisions and a summary of changes to assist in its review. The board's review and approval of bylaw changes should be clearly evident in board meeting materials and minutes.

- ***Maintenance:*** **Are effective processes in place to periodically review and update bylaws to ensure they remain current, relevant, and in compliance with regulatory requirements?** The institution should establish processes for maintaining bylaws. This should include an expectation that all bylaws be periodically reviewed to ensure they remain relevant. Bylaws may need updating to address changes in environmental conditions, organizational structure, regulatory requirements, or business practices. Bylaw administration should also address the approval process, including stockholder votes when required. Most bylaws can be modified by the board under the authorities granted to it by stockholders. However, some bylaws may require a stockholder vote to make a change. Additionally, there are regulatory requirements for a stockholder vote on certain bylaws. For example:

    - Capital (FCA Regulation 615.5220 and Section 4.3A of the Farm Credit Act of 1971, as amended)
    - Regional elections (FCA Regulation 615.5230(b))
    - Special class of stock when commencing termination of System status (FCA Regulation 611.1210(f))

- ***Implementation:*** **Are processes in place to implement bylaw changes and ensure they are accomplishing intended objectives?** Processes should be in place to ensure compliance with bylaws and accomplishment of intended objectives. Often, bylaw changes will create the need for changes to policies, procedures, or internal controls. The board and management should update any applicable guidance and controls to ensure the bylaw change is effectively implemented. Training should also be provided to staff on bylaw changes that may impact them, as well as stockholder communication, if necessary. Results from our examination of individual bylaws and other related examination work can provide insight into the effectiveness of bylaw administration and implementation.

- ***Internal Audit:*** **Is bylaw administration appropriately considered in the audit universe and audited periodically?** Bylaw administration should be considered for audit periodically based on risk assessed, similar to other auditable areas. Refer to the *Audit* procedure for examining bylaw administration audits.

7. Policy Administration:

Determine if processes for developing, maintaining, and implementing board policies are adequate.

Guidance:

An essential role of the board is to guide and direct operations through development, maintenance, and implementation of board policy. Board policies (and management's implementing procedures) need to be consistent with regulatory requirements and the institution's business model, risk appetite, and operating environment. Effective policy administration includes board development and communication of guidance and expectations necessary for safe and sound operations. The guidance below outlines important aspects of an effective policy administration process. Refer to The Director's Role for additional guidance and criteria on the board's policy-making role.

Note: This examination procedure focuses on policy administration and not on individual policies. Individual policies are addressed in the applicable procedures throughout the Examination Manual. For example, we address the examination of the Internal Control policy in the *Internal Control Policy* procedure. Examiners should consider the results from examining individual policies when concluding on the effectiveness of policy administration.

Evaluative questions and items to consider when examining policy administration include:

- ***Board Direction and Involvement:*** **Is the board sufficiently involved in the policy administration?** The board needs to be involved in the development, review, and approval of new and revised policies. Board direction on policy administration processes should be addressed and documented in a policy or other guidance document. While management typically drafts policies and related revisions, the board needs to provide direction on policy content and ensure it understands each policy. If needed, the board may consider obtaining assistance from an external subject matter expert on areas that are more complex or new to the institution. Management often provides the board a redline copy of proposed policy revisions or a summary of changes to assist in its review. The board's review and approval of new or revised policies should be evident in board meeting materials and minutes.

- ***Development Considerations:*** **Does the board and management consider the appropriate information when developing and revising policies?** There are many considerations when

determining the need for, and content of, a board policy. Policy content should be tailored to the institution's unique characteristics and operating environment. The following are common examples of information sources the board and management should consider:

- Statutory or regulatory requirements (certain statutes and regulations require policies governing specific activities or programs; these are identified in FCA's Board Policies and Charters document).
- Charter and bylaws.
- Strategic, operational, and capital plans.
- Culture, philosophy, and risk appetite.
- Condition, performance, and risk bearing capacity.
- The current operating environment (internal and external), emerging risks, scope of operations, and operational complexity.
- Management and staff capabilities and expertise.
- Industry standards and other authoritative guidance or information.
- Existing policies (to avoid inconsistency or redundancy between policies).

- ***Content and Structure:*** **Does the policy development process adequately address expectations on policy content and structure?** Board guidance on policy administration should clearly address expectations on policy content and structure. The following are common elements of an effective policy:
  - *Purpose* – A statement clearly articulating the policy's goals.
  - *Objectives* – Simple statements that outline what the policy intends to achieve.
  - *Operating Parameters* – Identification of parameters within which management and staff are expected to operate. Parameters should be consistent with sound business practices and applicable laws, regulations, and other guidance, such as generally accepted accounting principles or industry standards.
  - *Delegations* – Identification of authorities delegated to management and those retained by the board.
  - *Exceptions* – Direction on any allowable exceptions to the policy's requirements and the process for handling them.
  - *Reporting Requirements* – Expectations on management reporting to the board, including content and frequency of reports and responsibility for preparing the reports.

- ***Maintenance:*** **Are effective processes in place to periodically review, revise, and approve policies?** Board guidance on policy administration should address processes for maintaining policies to keep them current and ensure they are accomplishing their intended objectives. The board or its designated committee(s) should periodically review policies to determine if revisions are needed. Policy revisions may be needed to address changes in environmental

conditions, organizational structure, regulations, business performance, risk profile, internal controls, or the institution's programs or practices. To assist with monitoring for these types of changes and determining their impact on policies, it is beneficial to assign responsibility to members of management as policy content owners in their operational areas. While policies should be revised whenever needed, the board should define a frequency for periodically reviewing all policies. When setting this frequency expectation, the board may choose to establish a rotational schedule to review a group of policies each year. Board meeting minutes should document the board's review, discussion, and approval of policies (or reaffirmation if there are no revisions).

- ***Storage and Communication:*** **Are effective processes in place to store policies and communicate new or revised policies to staff?** The institution should have a storage (filing) system that provides easy access to board policies by board members, management, and staff. The board and management should also have a process to communicate new or revised policies throughout the organization and provide training, as needed, to ensure staff awareness and understanding.

- ***Procedure Updates:*** **Are effective processes in place to ensure procedures, processes, and controls are updated to reflect new or revised policies?** When policy changes are made or new policies are developed, management should review and revise, as needed, the related procedures, processes, and internal controls to ensure policy direction is effectively implemented. The institution may have a centralized process or control to ensure this process is completed, such as a designated person that oversees policy and procedure administration. Alternatively, the content owners (as discussed above) would need to ensure updates are made. Like policy changes, the institution should have a process to ensure these updates are communicated to staff, with training provided, as needed.

- ***Implementation:*** **Are processes in place to evaluate if policies have been appropriately implemented and are accomplishing intended objectives?** Processes should be in place to measure and monitor compliance with board-approved policies and accomplishment of intended objectives. This can be achieved with communications to the board through internal audit reports, policy exceptions reports, and other management reports in specific areas. This can also be completed as part of the routine policy review process. If the reports or reviews show policies (and related procedures) are not implemented correctly, applied uniformly throughout the organization, or achieving the intended results, the board should act to ensure policies are appropriate, understood, enforced, or revised, as warranted.

- ***Internal Audit:*** **Is policy administration appropriately considered in the audit universe and audited periodically?** Policy administration should be considered for audit periodically based on risk assessed, similar to other auditable areas. Refer to the *Audit* procedure for examining policy administration audits.

- ***Results from Examination of Individual Policies:*** **Did our examination of individual policies evidence effective policy administration?** Results from the examination of individual policies can provide insight into the effectiveness of policy administration. Individual board policies are addressed in the applicable procedures throughout the Examination Manual.

8. Internal Control Policy:

Evaluate the internal control policy for compliance with regulations and sufficiency of board direction over the internal control function.

Guidance:

A sound internal control environment and framework is a critical part of effective governance. Internal controls are the systems, policies, procedures, and processes established by the board and management to safeguard assets and limit or control risks. FCA Regulation 618.8430 requires each chartered System institution's board to adopt an internal control policy that provides adequate direction in establishing effective control over, and accountability for, operations, programs, and resources. An effective internal control policy should address the relevant aspects of the internal control environment and framework, including the audit and review programs.

Note: FCA's approach to examining internal controls is based on an ongoing risk assessment of the internal control environment and framework. This procedure focuses specifically on examining the internal control policy, which the board should use to capture and communicate the institution's general control framework. However, internal controls permeate each functional area of the institution. As such, more detailed procedures and control processes will typically be embedded in these functional areas. Accordingly, FCA's examination of specific internal controls occurs within each applicable Examination Manual topic area.

Evaluative questions and items to consider when examining the internal control policy include:

- ***Regulatory Compliance:*** **Does the policy sufficiently address regulatory requirements?** FCA Regulation 618.8430 requires the board to adopt an internal control policy and identifies specific items that must be included. These minimum items are summarized and explained below (note that specific details can be addressed elsewhere, such as other policies or procedures).

    - Direction to management that assigns responsibility for the internal control function in operational areas to an institution officer(s). The regulation specifically identifies the financial, credit, credit review, collateral, and administrative areas, but the institution should also address technology and any other substantive operational areas. While the board may delegate administration of internal controls to management, it retains ultimate accountability for the internal control environment. The institution may adopt an internal control framework to help manage and implement internal controls.

    - Adoption of internal audit and control procedures that evidence responsibility for review and maintenance of comprehensive and effective internal controls. Details on the key types of internal controls (e.g., separation/segregation of duties, training, management review, reporting, audit and review) can be addressed in the underlying procedures.

    - Direction for the operation of a program to review and assess the institution's assets. The policy must include standards that address the administration of this program, including:

        - Loan, loan-related assets, and appraisal review standards, including standards for scope of review selection and standards for workpapers and supporting documentation. An independent internal credit review (ICR) function (also known as internal review, audit, or asset review) is a critical credit control system. The ICR should provide the board an independent evaluation of credit administration practices, risk identification reliability,

and asset quality reporting accuracy.

- Asset quality classification standards to be used in accordance with a standardized classification system consistent among associations within a district and their funding bank. Institutions identify, measure, and report credit risks through various methods, such as the Uniform Classification System and risk ratings.

- Standards for assessing credit administration, including the appraisal of collateral. Credit administration involves the processes and controls a lender uses to make and service a loan until it is collected in full. FCA Bookletter BL-069 provides further guidance on our expectation that each System institution will continuously assess its lending and loan servicing controls to ensure controls remain effective and comply with FCA Regulation 618.8430.

- Standards for the training required to initiate the program to review and assess assets. Staff (or third parties) responsible for activities that are part of the program to review and assess assets should have the knowledge and expertise necessary to adequately perform these activities. Management should establish training programs to ensure staff maintain the necessary skills (e.g., conducting audits or reviews, assigning asset quality classifications, ensuring sound credit administration). Establishing standards for the training required to carry out these activities will help ensure the program provides a reliable assessment and control of credit and credit-related risks for the board to effectively carry out its governance and oversight responsibilities. If an activity is outsourced, management should perform adequate due diligence to ensure an appropriate level of knowledge and expertise exists.

  - The role of the Audit Committee in providing oversight and review of internal controls. Refer to the *Audit Committee* procedure in the *Audit & Review Programs* Examination Manual topic for guidance on examining Audit Committee oversight.

- ***Adequacy of Policy Direction:*** **Does the policy provide sufficient baseline direction for establishing effective internal controls?** While the policy might include all the elements required by FCA Regulations, this does not ensure the policy's effectiveness. If internal control weaknesses exist in areas covered by the internal control policy, examiners should evaluate the adequacy, effectiveness, or implementation of the policy and the institution's internal control program. Understandably, the policy cannot prevent all internal control breakdowns; however, it should provide adequate direction and detail to guide staff to carry out the controls. Some key considerations regarding adequacy of the policy direction include a commitment to competence in the control environment (e.g., trained, skilled, and accountable staff), a sound organizational structure, appropriate compensation and performance programs, clear segregation of duties, etc. Refer to the guidance on specific internal controls referenced above and contained throughout the Examination Manual and consider the results from related examination activities when concluding on internal control policy guidance.

9. Board Reporting Processes:

Evaluate the adequacy of board reporting processes.

Guidance:

Reporting to the board is crucial for enabling directors to carry out their duties. Effective reporting processes help ensure the board has adequate information to monitor performance, facilitate effective and informed decision-making, and ensure board direction is implemented. Reporting also provides directors insight into operations and culture and an opportunity to affirm or challenge management assertions.

Note: This examination procedure focuses on board reporting processes and not on specific board reports. Examiners evaluate adequacy of specific board reports in the applicable procedures throughout the Examination Manual. For example, we address the examination of capital reporting in the *Capital Management* Examination Manual topic. Examiners should consider the results from examining reports in the different topical areas when concluding on the effectiveness of board reporting processes.

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

- ***Board Direction:*** **Does the board provide sufficient guidance on board reporting processes and expectations?** Board reporting processes and general expectations on reporting should be addressed in a board reporting policy or other guidance document. While various operational policies would address specific reporting expectations, this board reporting policy or guidance document should summarize what is to be reported to the board. For example, as outlined in The Director's Role, board reporting should address information required by board policy, updates on business plan components, and at least a quarterly review of institution performance. The guidance should also assign management responsibility for reporting and address items such as accuracy, timeliness, format, and distribution of reports, as discussed below.

- ***Accuracy and Timeliness:*** **Do reporting processes ensure that reports provide accurate, complete, and timely information to the board?** The board's guidance on reporting processes should communicate expectations for accurate, complete, and timely information. Accurate and complete information is necessary for the board to make informed decisions. Timely information helps to ensure report content is relevant and aides in effective oversight. Timeliness is also important to ensure directors have enough time to review the information and prepare for meetings. For example, sending board packets out that include several hundred pages a few days before a meeting may not provide directors with enough preparatory time.

- ***Format and Distribution:*** **Are board reports formatted and distributed effectively and securely?** The board's guidance on reporting processes should ensure information is presented in an easily understood and secure format to facilitate effective oversight. The board should clearly define the amount and type of reports it wants in board materials as well as how the materials are presented (e.g., executive summaries, detailed reports, and dashboards). Reports should summarize and highlight key information to help directors focus their attention on material matters. Too much detail and volume can be overwhelming

or make it difficult to interpret and conclude. More information is not necessarily better. Management should coordinate closely with the board to ensure directors receive the information needed. Additionally, the board and management need to ensure reports and related information are distributed to directors in a secure manner. Guidance on reporting processes should address systems and controls to maintain the security and confidentiality of this information.

- ***Internal Audit:*** **Are board reporting processes appropriately considered in the audit universe and audited periodically?** Board reporting processes should be considered for

  audit periodically based on risk assessed, similar to other auditable areas. Refer to the *Audit* procedure for examining board reporting audits.

- ***Results from Examination of Board Reports:*** **Did our examination of individual board reports evidence effective board reporting processes?** Results from the examination of individual board reports can provide insight into the effectiveness of board reporting processes. Individual board reports are addressed in the applicable procedures throughout the Examination Manual.

10. Corrective Action Processes:

Evaluate corrective action processes and controls to ensure timely followup, reporting, and resolution of identified weaknesses.

Guidance:

Institutions need an effective corrective action process to adequately and timely resolve weaknesses identified in audits, reviews, and examinations. The process should be addressed in guidance documents and include controls such as tracking tools and reporting expectations that ensure weaknesses and their underlying causes are corrected. Management is typically responsible for identifying and implementing specific corrective actions in response to audit, review, and examination reports. However, the board is ultimately accountable for overseeing the corrective action process and ensuring timely and effective resolution of identified weaknesses. The board may delegate oversight of the corrective action process to a committee, such as the Audit Committee.

Evaluative questions and items to consider when examining corrective action processes and controls include:

- ***Guidance:*** **Does the institution have adequate guidance on the corrective action process?** Policies, procedures, or other guidance should provide direction and expectations to guide an effective corrective action process. To maintain independence and objectivity, the Chief Audit Executive (CAE) or designated audit coordinator should be responsible for tracking corrective action plans, verifying actions taken, and reporting to the board. Effective guidance should address the following items:

  - Board and management roles and responsibilities.

  - Processes, expectations, and responsibilities for preparing corrective action plans, tracking and confirming corrective action completion, verifying effectiveness of actions taken, and other corrective action plan processes.

- Time frames for preparing a response to audit, review, and examination findings, providing that response to the board, and providing progress reports on the status of corrective action completion.

- How the corrective action tracking tool will be used in reporting to the board and which items from audits, reviews, and examinations will be included (e.g., requirements, recommendations, suggestions, observations). Guidance should also consider reporting expectations when management's response to a finding is to take no action and accept the risk.

- ***Tracking Tool:*** **Does the institution have a sufficient corrective action tracking tool?** The institution's corrective action tracking tool should support an effective process for resolving issues identified in audit, review, and examination reports. The tool should be implemented in accordance with the institution's guidance for corrective action processes, with reasonable controls to ensure integrity of the information. An effective tracking tool should address items such as:

  - The corrective action item identified in the audit, review, or examination report.

  - Planned actions to correct the weakness and its underlying cause, with enough detail to understand the actions to be taken.

  - Party responsible for correcting the weakness.

  - Time frame or due date for completion (which can also help establish prioritization of corrective action responses).

- ***Board Reporting:*** **Is reporting timely, accurate, and sufficient for the board to monitor and oversee resolution of audit, review, and examination weaknesses and their underlying causes?** As discussed in The Director's Role, the board should oversee and track progress in correcting weaknesses. This can be achieved through effective and timely reporting processes. Board reporting should follow defined reporting expectations. A corrective action plan should be provided shortly after the audit, review, or examination; however, the CAE or audit coordinator should also provide ongoing corrective action progress reports at least quarterly for the board to monitor resolution of corrective action items. Progress reports should inform the board of material modifications to, or deviations from, planned corrective actions. This includes delays in established corrective action plan time frames or due dates. Progress reports should include enough detail to hold management accountable for timely resolution.

- ***Effectiveness:*** **Are corrective action processes effective in resolving audit, review, and examination weaknesses in a timely and satisfactory manner?** Results from FCA's oversight and examination work and the institution's internal audit and review activities should provide insight into the effectiveness of corrective action processes. Concerns with resolution of matters requiring attention from FCA examination reports or findings in audit or review reports could indicate weaknesses in the process that warrant investigation. If examination work in the *Audit* procedures in applicable Examination Manual topics identifies inadequate or untimely resolution of weaknesses, examiners should further evaluate 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 corrective action process, including board oversight of the process.

- ***Internal Audit:*** **Are corrective action processes appropriately considered in the audit universe and audited periodically?** Corrective action processes should be considered for audit periodically based on risk assessed, similar to other auditable areas. Refer to the *Audit* procedure for examining corrective action processes audits.

11. Board Committees:

Evaluate the use of board committees to provide effective board oversight.

Guidance:

Board committees (e.g., audit, governance, risk, compensation) are an important component of the board's governance structure. Board committees can help boards carry out oversight responsibilities and function more effectively as outlined in The Director's Role. It is the board's responsibility to determine which committees it needs to govern effectively. To cover a wider range of issues with greater depth of analysis, the board can delegate work to a committee and enhance the board's overall effectiveness. Through committees, the directors are better able to focus their time and attention on matters where they have greater expertise or experience. Committee meetings encourage directors to thoroughly consider issues, promote more candid discussions, and gain better insight into certain activities. While board committees act on behalf of the board, the entire board remains accountable for the decisions and actions of board committees. Refer to The Director's Role for additional guidelines for board committees.

Evaluative questions and items to consider when examining board committees include:

- ***Committee Structure:*** **Has the board appropriately established a committee structure based on its governance needs?** The appropriate governance and committee structure is an important board decision that will vary based on each institution's needs. The board should clearly understand and define the responsibilities of each designated committee. Laws and regulations mandate some committees such as the Audit Committee, Compensation Committee, and Credit Review Committee. In addition, we often see governance, executive, risk, or compliance committees. As the institution's complexity and risk profile increases, additional committees may be necessary for the board to provide effective oversight. Similarly, changing conditions may warrant additional committee member skills or expertise. The board may also use ad hoc committees to deal with certain situations that may arise such as an investigative committee. However, it is important to consider that too many committees can create competing demands and the potential for duplication and confusion about responsibilities.

- ***Charters:*** **Does each board committee have an effective charter?** Each committee should have a written charter that defines the committee's responsibilities, size, member qualifications, authorities, and independence. The charter should establish requirements for meeting frequency, conduct, attendance, minutes, reporting, and advisor use. The charter should also address annual performance evaluations of the committee as well as ongoing training for committee members. Committee performance evaluations can be separate or part of the overall board evaluation process. The board should review the written charters at

least annually. The board should consider disclosing written charters, as appropriate (e.g., on websites, in proxy statements, policy manuals) to improve the transparency of the board's decision-making processes.

- ***Membership and Training:*** **Is committee membership and training appropriate?** The board should assign directors to committees that align with their skills and experience. In some circumstances, regulations require directors to have specific qualifications to serve on certain committees (e.g., Audit Committee). Committee members should receive the training they need to carry out their duties, especially for board committees requiring specialized skills or knowledge. The board should also consider directors' time commitments when allowing participation on multiple committees to avoid overburdening any single director. However, some committee overlap is beneficial in integrating board activities. With smaller boards, directors will likely need to serve on multiple committees. The board should find the right balance between maintaining institutional knowledge and gaining new perspectives. Periodically rotating committee membership may achieve optimal objectivity, but frequent rotation may adversely affect the committee's knowledge base and effectiveness.

- ***Effectiveness:*** **Does the committee effectively carry out all duties assigned by its charter?** Committee members should be engaged and attentive to the responsibilities defined in the committee charter. The committee should sufficiently document evidence of engagement and effectiveness in committee materials and reports to the full board. Committees should receive the support and resources they need to carry out their duties. The board should have an established system to ensure the committee carries out its responsibilities according to its charter.

Note: Examiners should address the effectiveness and regulatory compliance of Audit, Compensation, and Credit Review Committees in the *Audit Committee* procedure in the *Audit and Review Programs* Examination Manual topic, the *Compensation Committee* procedure in the *Human Capital Management* Examination Manual topic, and the *Notice of Action and Review* procedure in the *Borrower Rights* Examination Manual topic, respectively.

12. UBEs:

Evaluate the adequacy of guidance and controls for administering the use of unincorporated business entities (UBEs) and complying with FCA Regulations and guidance.

Guidance:

FCA Regulations in Part 611, Subpart J allow institutions to organize or invest in UBEs for certain designated purposes. Institutions must submit to FCA's Office of Regulatory Policy either a notice or a request for approval when organizing or investing in a UBE, as required by FCA Regulations 611.1154 and 611.1155, respectively. Guidance on submitting this information to FCA is outlined in an Informational Memorandum titled Guidelines on Submissions of Notices to FCA and Requests for FCA Approval of Unincorporated Business Entities dated July 30, 2013. In addition, institutions that use UBEs should have sufficient guidance and controls for administering UBE activities. Evaluative questions and items to consider when examining UBE administration include:

- ***Guidance and Controls:*** **Are guidance and controls sufficient to ensure compliance with FCA requirements on the use of UBEs?** Guidance and controls should be in place for

institutions that have used or plan to use UBEs. The level of guidance and controls should be commensurate with the extent of UBE use. For example, institutions that only use UBEs infrequently for acquired properties would not be expected to have the same level of guidance and controls as institutions that make more extensive use of UBEs. Additional controls could include separation of duties, multiple levels of approval, extensive reporting, and training and expertise requirements. For institutions that have used or plan to use UBEs, guidance and controls should specifically address and ensure compliance with the following regulatory requirements:

  - Compliance with the general restrictions and prohibitions on the use of UBEs as outlined in FCA Regulation 611.1153.
  - Submission of the required notice or request for approval before organizing or investing in a UBE as outlined in FCA Regulations 611.1154 and 611.1155.
  - Adherence to all FCA conditions of approval on individual UBEs.
  - Maintenance of documents necessary to protect the institution's interest in each UBE as required by FCA Regulation 611.1156(a).
  - Divestiture as soon as practical of its interest in UBEs as required by FCA Regulation 611.1156(b).
  - Disclosure of UBE investments and business activity in the annual report as required by FCA Regulation 611.1157(a). (Note: UBEs need to be reported in the annual report until dissolved.)
  - Periodic reports to FCA on any equity investment in a UBE or UBE status (as directed by FCA) as required by FCA Regulation 611.1157(b).
  - Timely reporting to FCA on dissolution of UBEs that it controlled as required by FCA Regulation 611.1157(c). (Note: The controlling institution should also be notifying associated institutions of dissolution.)

- ***Grandfathered UBEs:*** **Has the institution complied with the requirements in FCA Regulations 611.1158(b) and (c) for UBEs that existed prior to July 22, 2013?** Grandfathered UBEs remain subject to their conditions of approval and the same ongoing requirements, disclosures, and reporting as other UBEs. In addition, changes to a grandfathered UBE or an institution investing for the first time into a grandfathered UBE are subject to the notice and approval requirements of the regulations.

- ***Reporting:*** **Do FCA and the board receive the required and appropriate reporting on UBEs?**

  - *Reporting to FCA* – FCA Regulations 611.1157(b) and (c) require periodic UBE reports (as directed by FCA) and timely reporting of UBE dissolution, respectively. FCA may request periodic reports on any equity investment in a UBE to assist in regulatory oversight. To report dissolution, institutions should send a letter (via mail or email) to FCA's Office of Regulatory Policy describing the termination along with the Articles of Termination or equivalent documentation for the state in which the UBE was established. The notice of dissolution by the controlling institution should list all the associated institutions involved in the UBE. If the notification does not list each institution, then each institution needs to separately notify FCA of the dissolution. If

an individual institution is divesting of a UBE, then that institution needs to notify FCA separately.

- *Board Reporting* – Similar to the extent of guidance and controls, the amount and frequency of board reporting should be commensurate with the extent of UBE use. Reporting should enable the board to monitor UBE activities and investments for compliance with regulations and the institution's guidance and to ensure the

  objectives of each UBE are being achieved. Board reporting should occur in accordance with board policy.

13. Audit:

Determine if the institution conducts an effective audit (scope, reporting, and followup) of direction and control of operational areas.

Guidance:

The internal audit and review program is a key mechanism for ensuring effective direction and control of operations and compliance with regulatory requirements. The internal auditor or other qualified, independent party should review the adequacy of processes to ensure compliance with applicable criteria. The audit risk assessment and scope should address direction and control of operational areas, and audit or review frequency should be commensurate with the complexity of the institution's operations and risk profile. A reliable audit program provides the board reasonable assurance that direction and control of operations is sound and that reporting is complete and accurate.

Note: This procedure focuses on evaluating the reliability and effectiveness of internal audits and reviews in this topical area. Refer to the *Audit & Review Programs* topic in the Examination Manual for guidance on examining the overall internal audit and review program.

Evaluative questions and items to consider when examining the audit or review of direction and control of operations include:

- ***Audit Coverage:*** **Is there periodic audit or review coverage of direction and control of operational areas?** Audit or review coverage and frequency 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 or review scope and depth sufficient to conclude on the adequacy, completeness, and timeliness of direction and control of operational areas and related processes?** The scope and depth of work, including transaction testing, 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 should be documented and consistent with the approved audit or review plan and engagement contract (if applicable). Audit or 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 audit plan. For example, 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 materially from the original planned scope, internal audit should notify the board (or Audit Committee, if so delegated) of the reasons for the change. Specific items that should be considered in the audit or review scope include:

- Policies and procedures for major direction and control of operational areas, including:
  - Enterprise risk management
  - Model risk management
  - Third-party risk management
  - Stress testing framework
  - Cooperative principles
  - Policy and bylaw administration
  - Board reporting processes
  - Corrective action processes
  - Board committees
  - Unincorporated business entities (if applicable)
- Compliance with direction and control of operations-related policies, procedures, FCA Regulations, and other FCA guidance.
- Monitoring and control processes (e.g., reporting, management oversight, delegated authorities, separation of duties, staffing, management information systems).
- Fraud-related threats and vulnerabilities, as well as anti-fraud controls.

- ***Reliability of Results:*** **Did FCA identify any concerns with audit or review reliability?** It is important to understand the scope and depth of the audit or review being examined, as discussed above, when evaluating audit or review reliability. With this understanding, the following are key considerations when evaluating the reliability of audit or review results:
  - *FCA Testing* – Evaluate the reliability of internal audit or review work by comparing the results to FCA's examination results in this area. This 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). In addition to the audit or review report, examiners should request and review the workpapers and hold discussions with the auditor to obtain a more thorough understanding of 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.
  - *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 audit or review being examined as part of determining the reliability of results.

- *Institution Review of Work Performed* – The institution should complete an independent review of the workpapers to ensure audit or 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 Chief Audit Executive (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 or review reliability.

- ***Reports:*** **Does the internal audit or review report sufficiently communicate direction and control of operational area review results and recommendations, if applicable?** Examiners should consider the following when evaluating the audit or review report:
  - Is the report prepared and communicated in accordance with the institution's guidelines?
  - Is an executive summary or overview included to provide the board with a general conclusion on audit or review results?
  - Is the report accurate, concise, supported, and timely in communicating the audit or review objectives, scope, results, conclusions, and recommendations? (IIA Standards 2330, 2400, 2410, 2420, 2440, and 2450)
  - Are conclusions and recommendations realistic and reasonable, with material and higher risk issues clearly identified and prioritized?
  - Are conclusions and recommendations supported by convincing evidence and persuasive arguments (condition, criteria, cause, and effect)?
  - Do results in the workpapers align with report conclusions?
  - Does the report conclude whether the institution adheres to policies, procedures, and applicable laws or regulations, and whether operating processes and internal controls are effective?
  - Does the report address potential vulnerabilities to fraud, if applicable?

- ***Corrective Action:*** **Are management responses to audit or review findings in this area 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, there should be a reasonable, complete, and timely management response to the audit or review report. 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 the audit or review did not sufficiently identify 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.