

## MANAGEMENT AND INTERNAL CONTROL EVALUATION

### Core Analysis Decision Factors

Examiners should evaluate the Core Analysis in this section to determine whether an Expanded Analysis is necessary. This module is intended to incorporate and summarize the findings from all of the completed ED Modules for a given examination. Click on the hyperlinks found within each of the Core Analysis Decision Factors to reference the applicable Core Analysis Procedures.

**Do Core Analysis and Decision Factors indicate that risks are appropriately identified, measured, monitored, and controlled?**

- C.1. Does the board adequately supervise the affairs of the bank and provide for management depth and succession? Refer to Core Analysis [Procedures #1-20](#); [Procedure #23](#); [Procedures #27-29](#); & [Procedure #43](#).**
- C.2. Has management established an adequate control environment throughout the organization? Refer to Core Analysis [Procedures #24-25](#); [Procedure #28-29](#); [Procedures #40-42](#); & [Procedures #44-47](#).**
- C.3. Is management responsive to recommendations from auditors and supervisory authorities? Refer to Core Analysis [Procedure #26](#).**
- C.4. Are insider activities appropriate? Refer to Core Analysis [Procedures #30-31](#).**
- C.5. Are management capabilities sufficient for the size, activities, and condition of the bank? Refer to Core Analysis [Procedures #21-22](#).**
- C.6. Does management identify and assess the major risks confronting the bank? Refer to Core Analysis [Procedures #33-42](#).**
- C.7. Are policies and procedures generally adequate given the size and complexity of the bank? Refer to Core Analysis [Procedure #20](#); [Procedure #25](#); & [Procedure #27](#).**
- C.8. Do management information systems provide effective internal communication of the bank's risks? Refer to Core Analysis [Procedures #48-49](#).**
- C.9. Are appropriate governance systems in place to monitor the activities of the bank? Refer to Core Analysis [Procedure #32](#) & [Procedure #50](#).**

## **MANAGEMENT AND INTERNAL CONTROL EVALUATION**

### **Core Analysis Procedures**

*Examiners are to consider these procedures but are not expected to perform every procedure at every bank. Examiners should complete only the procedures relevant for the bank's activities, business model, risk profile, and complexity. If needed, based on other identified risks, examiners can complete additional procedures. References to laws, regulations, supervisory guidance, and other resources are not all-inclusive.*

#### **Preliminary Review**

1. Review board, committee, and shareholder meeting minutes since the last examination and the most recent and year-end board packages to assess board supervision. Consider the following items:
  - Director attendance,
  - Changes in control,
  - Board independence from management,
  - Dominant control by a board member, shareholder, or management,
  - Significant changes in the direction or activities of the bank,
  - Significant changes in the bank's economic or competitive environment,
  - Adequacy of management information systems,
  - Implementation and maintenance of adequate policies, and
  - The bank's strategic plan.
  
2. Review changes in management or the directorate since the last examination. Assess compliance with rules concerning notification of changes in executive management.<sup>1</sup>
  - Consider why changes were made or are planned.
  - Assess the effect of changes on bank operations or risk profile.
  - Review biographical information for new executive officers and directors.
  - Identify potential management interlocks.<sup>2</sup>
  
3. Review prior examination reports, workpapers, and correspondence for comments regarding board supervision, management, and internal controls.

#### **Board and Management Supervision**

4. Review the charter, by-laws, and other related documents to understand the governance framework for the board. Consider the following:

<sup>1</sup> FRB: Section 914 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989. FDIC: Section 32 of the Federal Deposit Insurance Act (FDI Act)

<sup>2</sup> FRB: 12 CFR Part 212; FDIC: 12 CFR Part 348

- The number of directors;
- Qualifications or restrictions for directors, including the chairman of the board;
- Mandatory retirement age, if any, for board members;
- Advisory Directors or Advisory Board;
- Directorate nomination and election process;
- Required committee structure; and
- Required frequency of board and committee meetings.

5. Assess the composition of the board of directors. Consider the following:

- The number of independent directors;
- Involvement of the chairman in day-to-day operations;
- The number of years each member has served on the board; and
- The business, industry, or financial expertise of the board.

6. Determine whether the board has an effective process to identify, nominate, and select qualified individuals.

7. Determine whether the organization provides new board members with an overview of their fiduciary responsibilities and opportunities for ongoing training.<sup>3</sup>

8. Assess the board's ethics program or code of conduct.<sup>4</sup> Consider the following:

- Application to all board members, officers, and employees;
- Internal guidelines regarding conflicts of interest, periodic training, and acceptable and unacceptable practices; and
- Documentation concerning deviations from policy and associated action.

9. Assess the strategic plan and the planning process. Consider the following:

- The planning time horizon;
- The bank's condition, risk profile, and business model;

<sup>3</sup> FDIC: Director responsibilities are discussed in FIL-87-92: *Statement Concerning the Responsibilities of Bank Directors and Officers* and in the *Pocket Guide for Directors*.

<sup>4</sup> FDIC: An effective ethics program typically contains the elements referenced in FIL-105-2005: *Guidance on Implementing an Effective Ethics Program*. Also consider Statement of Policy: *Guidelines for Compliance with Federal Bank Bribery Law*.

- **Current and future operating environment;**
- **Sufficiency of financial and managerial resources relative to risk appetite;**
- **Appropriateness of assumptions;**
- **Communication of goals throughout the organization; and**
- **Ongoing monitoring processes.**

**10. Determine whether the board is actively involved in the selection and retention of the chief executive officer (CEO) and other executive officers, and consider whether the board regularly assesses executive officers' performance.**

**11. Assess the talent development and succession planning process relative to the bank's size, complexity, and business model.<sup>5</sup> Effective planning processes typically consider the following:**

- **All key positions,**
- **Internal and external sources of talent,**
- **Short- and long-term planning horizons, and**
- **Periodic reviews and updates.**

**12. Assess board involvement, either directly or through a designated committee, related to compensation issues. Consider whether the board:**

- **Approves the compensation of senior executives;**
- **Ensures that incentive compensation arrangements for covered employees are appropriately balanced and do not jeopardize the safety and soundness of the institution; and**
- **Re-evaluates compensation when employee decisions lead to adverse financial outcomes.**

**13. Evaluate board and management reliance on external advisors or consultants.**

**14. Assess the board and management committee structures. Consider the following:**

- **Selection process for committee members;**
- **Rotation requirements;**
- **Selection of committee chair;**
- **Meeting frequency and attendance;**
- **Meeting agendas and minutes;**
- **Quality and timing of information flows from committees to the full board; and**

<sup>5</sup> Succession plans may be formal or informal.

<ul style="list-style-type: none"><li>• Need for additional committees.</li></ul>
<p><b>15. Assess whether committee charters adequately address financial and non-financial risk governance.</b></p> <p>Consider whether charter elements:</p> <ul style="list-style-type: none"><li>• Delineate a committee's size, responsibilities, and membership qualifications;</li><li>• Define oversight responsibilities of risk management policies and practices;</li><li>• Outline board responsibilities to sanction, review, and amend committee practices;</li><li>• Articulate the board's role and responsibility in establishing and reviewing risk levels;</li><li>• Identify metrics for assessing and reporting risk levels relative to defined risk thresholds; and</li><li>• Provide for ongoing dialogue between board and management regarding risk management practices.</li></ul>
<p><b>16. Assess the process for setting board and committee meeting agendas, and evaluate the appropriateness, accuracy, completeness, and timing of information received prior to meetings.</b></p>
<p><b>17. Determine whether the board established and communicated a whistleblower process that allows employees, vendors, and customers to anonymously report concerns to the board or audit committee.<sup>6</sup></b></p>
<p><b>18. Determine whether the board of directors, its committees, and executive management periodically conduct self-assessments of their performance. Assess the effectiveness of these reviews.</b></p>
<p><b>19. Evaluate the reasonableness of compensation paid to the directorate. Consider the following:</b></p> <ul style="list-style-type: none"><li>• Compensation or fees paid on a per meeting attended, annual, or other basis;</li><li>• Additional compensation for committee meetings;</li><li>• Compensation basis (cash, stock, stock option, or other basis);</li><li>• Deferred or other benefits; and</li><li>• Existence of performance-based compensation.</li></ul>
<p><b>20. Evaluate policies governing compensation programs. Effective compensation programs are typically established by written policies that address base pay and performance-based compensation arrangements. Areas of consideration include:</b></p>

<sup>6</sup> FDIC: Consider FIL-80-2005: *Fraud Hotline: Guidance on Implementing a Fraud Hotline*.

- **Cash and noncash payments;**
- **Equity compensation (e.g., stock options, stock appreciation rights, restricted stock or stock units);**
- **Deferred compensation and supplemental retirement plans;**
- **Severance (golden parachutes and change-in-control payments); and**
- **Forfeitures and clawbacks.**

**21. Determine whether key executives have the appropriate knowledge, skills, and experience relative to the nature and scope of their responsibilities.**

**22. Identify and assess the influence exerted by any dominant official or policymaker.<sup>7</sup>**

**23. Determine whether the organizational structure is appropriate considering the size, complexity, risk profile, business model, and strategic plan.**

## **Control Environment**

**24. Determine whether the board implemented an effective internal control system and ensures all personnel understand the importance of internal controls. Effective control systems provide reasonable assurance that internal controls will prevent or detect:**

- **Materially inaccurate, incomplete, or unauthorized transactions;**
- **Deficiencies in the safeguarding of assets;**
- **Unreliable financial or regulatory reporting; and**
- **Deviations from laws, regulations, and internal policies.**

**25. Determine whether the bank has a policy that requires all officers and employees to be absent<sup>8</sup> from their duties for an uninterrupted period of not less than two consecutive weeks. Assess its adequacy.**

<sup>7</sup> The presence of a dominant official should not be viewed negatively or as a supervisory concern in and of itself. Rather, the presence of a dominant official coupled with other risk factors such as ineffective internal controls, lack of board independence or oversight, or engagement in risky business strategies may create regulatory concerns or require enhanced supervision.

<sup>8</sup> Absence may involve vacations, rotations of duty, or a combination of both activities. Such policies are highly effective in preventing embezzlements, which usually require a perpetrator's ongoing presence to manipulate records, respond to inquiries, and otherwise prevent detection. The benefits of such policies are substantially, if not totally, eroded if the duties normally performed by an individual are not assumed by someone else.

**26. Determine whether management takes appropriate and timely action to address recommendations by auditors and regulatory authorities.<sup>9</sup>**

**27. Determine whether the board, through effective monitoring and enforcement, restricts management's ability to override established policies and procedures.**

**28. Evaluate the incentive compensation arrangements for executive management and other employees (individually or as a group) whose activities may expose the institution to material risks.<sup>10</sup> When reviewing incentive compensation arrangements, consider:**

- The type, level, and significance of incentive compensation as part of the overall compensation model and its influence on the institution's risk profile;
- Board approval of executive compensation incentives;
- The use of golden parachute agreements;<sup>11</sup> and
- Incentive compensation issues identified during the mortgage banking review or compliance examinations (e.g., mortgage loan origination compensation (Regulation Z)).<sup>12</sup>

**29. Assess the reasonableness of individual compensation arrangements relative to services performed.<sup>13</sup>**  
Consider the following:

- The combined value of cash and noncash benefits;
- The compensation history of the individual and others with comparable expertise and responsibilities;
- The financial condition of the institution;
- Documentation of the board's review and consideration of compensation practices at comparable institutions;
- For post-employment benefits, the projected total cost and benefit to the institution;
- Connection between the individual and any fraudulent act or omission, breach of trust or fiduciary duty, or insider abuse;
- Bank purchases of life insurance for compensation purposes; and
- Any other relevant factors.

<sup>9</sup> Refer to the Internal and External Audit Evaluation module.

<sup>10</sup> Appropriate incentive compensation arrangements typically balance risks and rewards; reflect effective controls and risk management practices; and are supported by strong corporate governance. Refer to the Interagency Guidance on Sound Incentive Compensation Policies, issued June 21, 2010, for further discussion.

<sup>11</sup> FRB: SR-96-21; FDIC: FIL-66-2010, and 12 CFR Part 359.

<sup>12</sup> Examiners should be cognizant of loan originator compensation requirements (Regulation Z) and notify compliance examiners as appropriate.

<sup>13</sup> Compensation practices are assessed in the context of the Interagency Guidelines Establishing Standards for Safety and Soundness (FDIC: 12 CFR Part 364, Appendix A; FRB: 12 CFR Part 208, Appendix D-1), and Section 39 of the Federal Deposit Insurance Act.

<p><b>30. Determine whether adequate systems are in place to identify and mitigate self-serving practices or conflicts of interest. Consider compliance with applicable laws, and determine whether:</b></p> <ul style="list-style-type: none"><li>• <b>Insiders have undue influence over customer activities;</b></li><li>• <b>Insiders are lending personal funds to customers or borrowers;</b></li><li>• <b>Privileges or benefits given to insiders are commensurate with the services rendered;</b></li><li>• <b>Insiders are conducting excessive non-bank related business at the bank or are spending inordinate amounts of time away from the bank; and,</b></li><li>• <b>Transactions related to insiders' purchase or use of bank assets (such as other real estate, repossessed vehicles, equipment, or bank facilities) are appropriate.</b></li></ul>	
<p><b>31. Evaluate whether the board appropriately monitors and manages transactions between the institution and its directors, management, principal shareholders, and affiliates (collectively, affiliated parties). Effective measures typically ensure that:</b></p> <ul style="list-style-type: none"><li>• <b>Transactions between the institution and an affiliated party are sound, in the best interest of the institution, and appropriately documented; and</b></li><li>• <b>Exceptions to established policies and standards governing transactions with affiliated parties are legally permissible and appropriately approved and documented.</b></li></ul>	
<p><b>32. Determine whether (and if so, why) the external auditor or legal counsel changed since the last examination.</b></p>	
<h3>Risk Assessment</h3>	
<p><b>33. Review and assess internal risk assessments for all significant business activities. Effective risk assessment processes typically include the following:</b></p> <ul style="list-style-type: none"><li>• <b>An assessment of all material risks and compensating controls,</b></li><li>• <b>A requirement to report assessment results to senior management and board committees,</b></li><li>• <b>A requirement to update internal control risk-assessment methodologies as business activities and work processes change.</b></li></ul>	
<p><b>34. Determine whether management's risk-taking practices are conservative, moderate, or aggressive by assessing practices relating to loans; investments; asset/liability management; growth; nontraditional banking services; deposit structures, rates, and products; and other pertinent areas. Consider whether:</b></p> <ul style="list-style-type: none"><li>• <b>Internal controls sufficiently mitigate higher risk activities;</b></li></ul>	

- There are material changes in management's risk-taking practices (e.g., changes in deposit products or funding sources; loan products, underwriting, or portfolio mix; investments, due diligence, or maturity distributions; and asset growth.)

**35. Evaluate the planning processes used throughout the institution. Consider findings from other ED modules, that may address the following:**

- The strategic plan, budget processes, profit plans, capital plans, and growth projections;
- Sensitivity analysis and stress testing in planning processes to identify potential vulnerabilities;<sup>14</sup>
- The adequacy of research regarding new strategic initiatives, such as new products and investments, branch expansions, acquisitions, or mergers; and
- The adequacy of contingency planning and business continuity planning that incorporates enterprise-wide considerations.

**36. Determine whether management adequately considers risks that influence the success or failure of established objectives. Generally, considerations include:**

- External sources of risk;
- Internal sources of risk; and
- The significance and likely impact of identified risks, compensating controls, and mitigating factors.

**37. Determine whether management monitors other risks arising from sources such as:**

- Media, internet, and social networks;
- Press releases and annual reports;
- Participation in or sponsorship of community events; and
- Other public venues.

**38. Consider whether management has an appropriate marketing and public relations strategy to manage business and operational risks.**

**39. Consider whether risks identified by examiners and external auditors differ from those identified by management.**

<sup>14</sup> Stress testing is considered a prudent practice to assist in the identification, measurement, and mitigation of risks whether on a whole bank or more targeted basis.

Control Activities
<p><b>40. Assess blanket bond insurance levels, considering:</b></p> <ul style="list-style-type: none"><li>• The financial condition of the bank, including capital levels and asset quality;</li><li>• Asset and deposit size and trends;</li><li>• The size of transactions, such as loans (in relation to legal lending limit) and wire transfers;</li><li>• Single-loss and aggregate liability levels;</li><li>• The effectiveness of internal controls;</li><li>• Whether areas of operations are rapidly expanding;</li><li>• The amount of cash, securities, and negotiable items normally held;</li><li>• The number, experience, and turnover rate of personnel;</li><li>• The extent of trust and merchant credit card activities;</li><li>• Data processing activities and internet presence;</li><li>• The presence of a dominant official or policymaker; and</li><li>• Previous fraudulent activities or claims and suspicious activity reports.</li></ul>
<p><b>41. Consider and assess other insurance policies, including Director and Officer and any excess employee fidelity policy.<sup>15</sup></b></p>
<p><b>42. Determine the reasons for any significant fidelity insurance claims.</b></p>
<p><b>43. Determine whether pre-employment and due-diligence practices for prospective directors, officers, employees, and significant third-party contractors address potential employment impediments.<sup>16</sup></b></p>
<p><b>44. Determine whether policies, procedures, and practices are adequate for the size, complexity, and risk profile of the bank by reviewing findings from other reviews completed during the examination.</b></p>
<p><b>45. Determine whether existing controls help ensure adherence to established internal policies and are reasonable in relation to risk exposures. Review the results of other reviews completed during the examination to determine the overall adequacy of internal controls.</b></p>

<sup>15</sup> For more information on Directors and Officers insurance policies see FIL-47-2013 (FDIC); SR 19-12 (FRB).

<sup>16</sup> For example, criminal convictions subject to Section 19 of the FDI Act (crimes related to dishonesty, fraud, and money laundering) and banking prohibition orders. All FDIC-insured institutions are subject to Section 19 of the FDI Act.

**46. Determine whether management maintains an effective system of controls and safeguards for activities that expose the bank to risk. Consider the following:**

- Authorization and reporting requirements;
- Data access controls; and
- Joint custody, dual control, and separation-of-duty arrangements.

**47. Determine whether management takes appropriate steps to comply with laws and regulations.**

### **Information and Communication**

**48. Evaluate information systems' ability to identify, capture, and report relevant internal and external information.**

- Determine whether the systems are commensurate with risk, complexity, and business model.
- Determine whether the board or management periodically evaluates the adequacy and accuracy of management information systems.
- Consider the accuracy of the Call Report.

**49. Evaluate whether information communication is sufficient for personnel to carry out their responsibilities.**

### **Monitoring**

**50. Determine whether systems exist to monitor material risks arising from all major activities in which the institution is engaged.<sup>17</sup> Assess risk monitoring with respect to the following:**

- Credit risk,
- Market risk,
- Liquidity risk,
- Operational risk,
- Legal risk, and
- Compliance risk.

<sup>17</sup> FRB: See SR 16-11

**End of Core Analysis. If needed, Continue to the Expanded and Impact Analyses.**