

Management and Internal Control Evaluation

Examiners should evaluate the above-captioned function against the following control and performance standards. The Standards represent control and performance objectives that should be implemented to help ensure the bank operates in a safe and sound manner, and that the entity's objectives are carried out. Associated Risks represent potential threats to the bank if the standards are not achieved and maintained. The Standards are intended to assist examiners in analyzing important functions that may warrant additional review. All of the following Standards may NOT need to be considered at every bank. Conversely, these do NOT represent all of the control and performance standards needed for every bank. Examiners should continue to use their judgement when assessing risk.

Standards	Associated Risks
MANAGEMENT AND CONTROL	
<p>An independent board assigns responsibility, delegates authority, and establishes policies to provide a basis for accountability and control.</p> <p>Lines of authority and responsibilities of management and employees are clearly stated and understood by all personnel.</p>	<p>The lack of independent oversight could result in a poor control environment.</p> <p>Inappropriate or deficient organizational structure may result in problems going uncorrected.</p>
<p>The board and executive management have the required knowledge, experience, and training to perform their duties.</p> <p>The board has a management succession plan, either formally or informally.</p>	<p>An unqualified board and management team may be ineffective.</p> <p>Inadequate management succession and depth may disrupt the bank's operations and adversely impact its financial condition.</p>
<p>The board uses an effective planning process and implements appropriate strategies.</p>	<p>An inadequate planning process may result in poor performance and missed opportunities.</p> <p>Management may be unresponsive to changes in economic, industry, and regulatory environments.</p>
<p>The board establishes control activities encompassing policies and procedures to ensure that directives are achieved.</p>	<p>The lack of control activities may prevent the realization of the organization's objectives.</p> <p>The bank may be exposed to greater risk if adequate policies and procedures addressing key risks are not implemented.</p> <p>The board and management may be unaware of non-compliance and corrective measures may not be initiated.</p>
<p>Management conveys the message that integrity and ethical values will be maintained.</p> <p>Management implements corrective actions recommended by auditors and supervisory authorities.</p>	<p>Self-serving practices and conflicts of interest could impair the bank's reputation and increase its exposure to legal risks and losses.</p>
<p>Management conducts risk assessments to identify key business risks.</p> <p>Management adheres to reasonable risk-taking practices.</p>	<p>Aggressive and uncontrolled risk-taking practices may increase the bank's exposure to risk.</p> <p>Internal controls may not be structured properly in areas of high risk.</p>

Standards	Associated Risks
Management maintains a system that effectively measures and monitors risks.	Capital, asset quality, earnings, and liquidity could be impaired by excessive risk.
<p>A process is in place to ensure relevant information is identified, processed, and reported by information systems.</p> <p>Information is communicated in an effective manner throughout the organization.</p>	Insufficient or untimely information prevents individuals from performing their duties effectively.
<p>Management, or a committee, monitor internal controls, including compliance with laws, regulations, and policy statements.</p> <p>Management, or a committee, enforces policies and procedures.</p> <p>The board establishes an effective audit program.</p>	<p>Ineffective monitoring could result in a poor internal control environment with a high probability of operating losses.</p> <p>Lack of policy and procedure enforcement could result in insufficient responses to problems and mismanagement of the bank.</p> <p>Operational weaknesses may not be found; financial or regulatory reporting may be unreliable; and compliance with laws, regulations, and internal policies may be jeopardized.</p>

Management and Internal Control Evaluation

Core Analysis Decision Factors

Examiners should evaluate Core Analysis in this section for significance and to determine if an Expanded Analysis is necessary. Negative responses to Core Analysis Decision Factors may not require proceeding to the Expanded Analysis. Conversely, positive responses to Core Analysis Decision factors do not preclude examiners from proceeding to the Expanded Analysis if deemed appropriate.

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

Core Answer: General Comment:(If any)

Core Analysis Decision Factors

C.1. Does the board adequately supervise the affairs of the bank and provide for management depth and succession?

C.2. Has management established an adequate control environment throughout the organization?

C.3. Is management responsive to recommendations from auditors and supervisory authorities?

C.4. Are insider activities appropriate?

C.5. Are management capabilities sufficient for the type, size, and condition of the bank?

C.6. Are the major risks that influence the success or failure of the bank identified and assessed?

C.7. Are policies and procedures generally adequate given the size and complexity of the bank?

C.8. Are adequate controls in place to ensure adherence to bank policies, and legal and regulatory requirements?

C.9. Are effective information and communication systems in place to enable personnel to carry out their duties?

C.10. Are appropriate systems, including audits, in place to monitor the activities of the bank?

Management and Internal Control Evaluation

Expanded Analysis Decision Factors

This section evaluates the significance and materiality of deficiencies or other specific concerns identified in the Core and Expanded Analyses.

Do Expanded Analysis and Decision Factors indicate that risks are adequately identified, measured, monitored, and controlled?

Expanded Answer: General Comment:(If any)

Expanded Analysis Decision Factors

E.1. Are management deficiencies or concerns immaterial?

Does management have the ability and commitment to implement corrective measures to effectively address deficiencies or concerns?

Management and Internal Control Evaluation

Consider the following procedures at each examination. Examiners are encouraged to exclude items deemed unnecessary. This procedural analysis does not represent every possible action to be taken during an examination. The references are not intended to be all-inclusive and additional guidance may exist. Many of these procedures will address more than one of the Standards and Associated Risks. For the examination process to be successful, examiners must maintain open communication with bank management and discuss relevant concerns as they arise.

IMPORTANT

The other examination modules contain specific procedures that will provide insight into management and internal controls in major risk areas. As such, the other examination modules MUST be completed prior to the overall assessment of management and internal controls. Coordinate procedures at the beginning of the examination to avoid duplication.

PRELIMINARY REVIEW

1 Review board and committee minutes since the last examination as well as the most recent and year-end board packages to determine the extent and adequacy of board supervision. Document important details. Consider the following items:

1 A Director attendance.

1 B Changes in control since the prior examination.

1 C Board independence from executive management.

1 D Dominant control by a board member, shareholder, or executive management.

1 E Significant changes in direction or activities of the bank.

1 F Adequacy of management information systems.

1 G Review and approval of policies.

1 H The bank's strategic plan.

2 Review changes in the bank's management or directorate since the last examination and review management succession plans. (Note: This plan can be either formal or informal.)

2 A Assess compliance with rules concerning notification of changes in executive management. (FRB: Section 914 of FIRREA, FDIC: Section 32 of the FDI Act).

2 B Assess the impact of management changes on bank operations.

2 C Obtain biographical information for new executive officers and directors.

3 Review prior examination reports, workpapers and correspondence for comments regarding management.

BOARD AND MANAGEMENT SUPERVISION

4 Determine if operational expertise is commensurate with the size, complexity, and risk profile of the bank.

5 Determine whether key executive officers are qualified and fulfilling their duties.

- 6 Determine whether the organizational structure is appropriate given:
 - 6 A The size and complexity of the bank,
 - 6 B The organization's strategic plan.
- 7 Determine to what extent management or the board relies on external advisors or consultants.
- 8 Determine if management has taken appropriate actions to comply with the Interagency Guidelines Establishing Standards for Safety and Soundness, FDIC: Part 364 Appendix A, or FRB: Appendix D, of Regulation H. (FDIC: Refer to RD memo 97-014)

CONTROL ENVIRONMENT

(Focuses on senior management's ability to establish a "tone from the top" regarding acceptable business practices, conflicts of interest, and expected behavior to ensure it is communicated and understood throughout the organization.)

- 9 Determine if management adequately addresses integrity in its code of conduct, ethics policy, and actions. Review and evaluate the following items:
 - 9 A Specific guidelines concerning conflicts of interest and periodic training, including acceptable and unacceptable business practices.
 - 9 B Suitable remedial action concerning departures from the policies.
 - 9 C Documentation concerning deviations from policies and documentation concerning remedial actions.
- 10 Determine if management takes adequate and timely corrective action to address recommendations by auditors and regulatory authorities.
- 11 Determine if the board of directors minimizes operating management's ability to override policies and procedures through effective monitoring and enforcement of established guidelines.
- 12 Determine the appropriateness of salary levels and compensation arrangements for both the board and executive management. Review the following areas:
 - 12 A Board approval of personnel compensation including individual salaries and benefits.
 - 12 B Approval of board members' compensation including individual fees and benefits.
 - 12 C Bank purchases of life insurance. (FDIC: Regional Director Memorandum Transmittal No. 96-084 provides general guidelines provided by OCC Bulletin 96-51, FRB: SR-96-21 Split Dollar Life Insurance at State Member Banks.)
 - 12 D Golden parachute agreements. (FDIC: Refer to Regional Director Memorandum Transmittal No. 96-026 and FIL-8-96 dated March 29, 1996, and February 16, 1996, respectively, FRB: SR-96-21 FDIC Final Rule Regarding "Golden Parachutes" and Indemnification Payments.)
 - 12 E Incentive-based compensation.
 - 12 F If necessary, supporting documentation from the board regarding compensation practices at comparable institutions, based on such factors as asset size, geographical location, complexity, and risk profile of the bank.

- 13 Determine if self-serving practices or conflicts of interest exist.
 - 13 A Determine if insiders have undue influence over customer activities.
 - 13 B Determine if insiders are lending personal funds to customers or borrowers.
 - 13 C Assess if privileges or benefits given to insiders are commensurate with the services rendered.
 - 13 D Determine if any insiders are conducting excessive non-bank related business at the bank or are spending inordinate amounts of time away from the bank.
 - 13 E Determine the appropriateness of any transactions related to insiders purchasing or using bank assets, such as ORE, repossessed vehicles, excess equipment, and bank facilities.
- 14 Determine if changes in external auditors or legal counsel occurred and why.

RISK ASSESSMENT

(Considers external and internal factors that could impact achievement of the bank's objectives, identifies and analyzes risks, and provides a basis for managing and reacting to changing conditions.)

- 15 Review management's risk-taking practices. Assess management's capabilities in the following areas: loans; investments; asset and liability management; growth; nontraditional banking services; deposit structure, rates, and products; and any other areas.
 - 15 A Determine if management's risk-taking practices are conservative, moderate, or aggressive.
 - 15 B Determine if the controls are in place to mitigate any concerns regarding risk-taking practices.
 - 15 C Determine if there are any material changes in management's risk-taking practices. For example, changes could occur in the following areas: loans to new borrowers, loan portfolio mix, securities portfolio maturity distribution, new loan products, or asset growth.
- 16 Determine if management plans effectively. Consider the following issues:
 - 16 A Strategic plan, budget process, profit plan, and growth projections.
 - 16 B Individuals involved with the planning process.
 - 16 C Reasonableness of assumptions.
 - 16 D Method of comparing actual performance against objectives.
 - 16 E Frequency of revisions.
 - 16 F Research efforts of new strategic initiatives such as new products and investments, branch expansion, and acquisitions and mergers.
- 17 Determine if management assesses risks that influence the success or failure of established objectives. A formal or informal risk assessment should consider the following areas:
 - 17 A External sources of risk such as:

- 17 A1 1. Technology changes.
2. Competitors' actions.
3. Economic conditions.
4. Political and regulatory conditions.
5. Accounting pronouncements.

17 B Internal sources of risk such as:

- 17 B1 1. Retention of key management and staff.
2. Availability of funds.
3. Information systems.
4. Corporate restructuring.
5. Rapid growth.
6. New products or business lines.

17 C The significance of the risks identified, the likely impact on the bank, and mitigating actions taken by management.

18 Determine if risks identified in the examination differ from risks identified by management.

19 Determine the appropriateness of blanket bond insurance levels. Consider the following items:

19 A Effectiveness of the bank's internal operations.

19 B Amount of cash, securities, and negotiable items normally held.

19 C Number, experience, and turn-over rate of personnel.

19 D Trust activities.

19 E Merchant credit card activities.

19 F Data processing activities.

19 G Previous fraudulent activities or claims.

20 Determine the adequacy of other policies including any excess employee fidelity policy.

21 Determine the reasons for any significant fidelity insurance claims.

CONTROL ACTIVITIES

(Encompasses a wide range of policies and the related implementation procedures that help ensure that management's directives are effected.)

22 Determine if policies, procedures, and practices are adequate for the size, complexity, and risk profile of the bank by reviewing findings from other modules completed during the examination.

23 Determine whether control activities are in place to ensure adherence to established policies, and review actions taken to address the related risks by reviewing the findings of the modules completed during the examination.

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

Core Analysis

- 24 A Authorization requirements.
 - 24 B Joint custody arrangements
 - 24 C Dual control.
 - 24 D Separation of duties.
- 25 Determine whether the bank has effective corporate business resumption and contingency planning.
- 25 A Consider if the bank maintains off-premise storage of back-up files for all critical records. (FFIEC Policy Statement on Contingency Planning for Financial Institutions.)
- 26 Determine if management takes appropriate steps to comply with laws and regulations.
- 27 Determine if management files appropriate suspicious activity reports, if necessary.

INFORMATION AND COMMUNICATION

(Includes identifying, capturing, processing, and reporting information by information systems. This information must be communicated throughout the organization.)

- 28 Determine whether information systems are in place to identify, capture, and report relevant internal and external information.
- 28 A Assess if the systems are adequate in the higher risk areas.
 - 28 B Determine if management regularly reviews information systems for accuracy.
 - 28 C Consider the adequacy of the Call Reports.
- 29 Evaluate whether communication of information is sufficient for personnel to carry out their responsibilities.

MONITORING

(Ensures appropriate procedures are in place to periodically evaluate the effectiveness of internal controls, to report deficiencies to appropriate personnel, and to modify policies and procedures.)

- 30 Determine if systems are in place to monitor material risks arising from all major activities in which the institution is engaged. Assess risk monitoring with respect to the following:
- 30 A Credit Risk.
 - 30 B Market Risk.
 - 30 C Liquidity Risk.
 - 30 D Operational Risk.
 - 30 E Legal Risk.
 - 30 F Reputational Risk.

AUDIT AND OTHER INDEPENDENT REVIEWS

(Note: For banks with formal internal audit departments, the following procedures should be considered. For those banks with either no audit function or with limited audit activity, monitoring, as defined above, can be evaluated through the other modules.)

31 Determine whether the internal audit function is sufficiently segregated from bank operations. Appropriate segregation is generally evidenced by the following items:

31 A The audit department is segregated from operations in the organizational structure.

31 B Audit staff is prohibited from performing any duties in lieu of operating personnel such as preparation of general ledger tickets, daily reconcilements, and dual control.

31 C Reporting procedures of the auditor are independent of the influence of operating personnel.

31 D The audit function reports directly to the board of directors and the audit committee, and the auditor periodically meets with them to review reports issued by the audit function.

32 Determine if there is a formal internal audit schedule in place to direct audit activities. The following are characteristics of a generally satisfactory plan:

32 A The audit schedule is reviewed and approved.

32 B All important bank functions and services are subject to audit.

32 C Audit procedures are updated as needed.

32 D The auditor periodically reports progress in completing the schedule to the board of directors.

32 E Starting dates and time intervals between audits are changed in order to avoid anticipation by those subject to audit.

33 Determine if internal audit records are adequate.

33 A A reasonable record retention schedule is maintained for audit records.

33 B Audit workpapers contain approval of significant deviations from audit procedures.

33 C Workpapers contain evidence that audit managers have reviewed the workpapers for findings and final conclusions.

33 D All significant and unresolved exceptions are noted in the workpapers and included in audit reports.

33 E Responsibility for maintaining the audit manual is assigned to appropriate staff.

34 Determine if the internal audit department's reporting procedures are adequate.

34 A The auditor submits formal reports to the board of directors or the appropriate committee regarding material weaknesses or other unsatisfactory matters.

34 B The board or appropriate committee supports the audit staff in resolving audit matters.

34 C Departmental managers commit to take specific actions to resolve matters noted in the audit reports.

34 D The audit reports include a summary of the effectiveness of controls in the department or function.

34 E The auditor maintains a formal record of all unresolved audit or regulatory exceptions and recommendations.

35 Determine whether audit staff's academic backgrounds and experience are sufficient for the size and complexity of the bank.

36 Review the bank's external audit program.

36 A If a bank is covered by Part 363 of the FDIC Rules and Regulations, or Appendix D of Regulation H, management is required to assess annually the effectiveness of its internal control structure and procedures for financial reporting and the bank's compliance with designated laws. Review the documentation maintained to assure management adequately assesses the internal control structure and compliance with laws.

36 B In banks that have chosen not to obtain an external audit, the board of directors should document its reasons including whether the auditing program provides sufficient coverage of areas of potential concern or unique risk. The examiner should review the minutes describing the board's consideration of this audit issue at each examination. If, in the judgement of the examiner, additional external audit coverage is warranted, specific suggestions for addressing these areas should be recommended; however, the lack of an external audit will not automatically result in negative comment.

36 C Determine if the audit program is in compliance with FRB Appendix D of Regulation H or FDIC Part 363, the Statement of Policy Regarding Independent External Auditing Programs of State Nonmember Banks.

Management and Internal Control Evaluation

Generally, procedures used in the Expanded Analysis should target concerns identified in the Core Analysis and Decision Factors. Expanded procedures associated with Core Analysis and Decision Factors of no concern need not be used. The flexible guidelines specified for the Core Analysis also apply here.

- 1 Determine why an ethics policy has not been adopted. Obtain management's response to examiner recommendations.
- 2 Determine the significance of insider abuses identified in the other modules.
- 3 Determine why the bank does not have fidelity insurance, and review the steps management is taking to mitigate the consequences of not having insurance coverage.

Management and Internal Control Evaluation

Impact Analysis reviews the impact that deficiencies identified in the Core and Expanded Analysis and Decision Factors have on the bank's overall condition. Impact Analysis also directs the examiner to consider possible supervisory options.

- 1 Determine whether management deficiencies or suspicious activities have resulted or could result in increased asset quality problems, deteriorated earnings, decreased capital protection, or undue risk to the bank.
- 2 Consider whether an informal or formal enforcement action is warranted, such as an MOU, a Cease and Desist Order, or a removal action. Advise the appropriate supervisory officials. (FDIC: Field Office Supervisor or Regional Office.)

CIVIL MONEY PENALTIES (FDIC)

- 3 Prepare recommendations for Civil Money Penalties, if appropriate. (FDIC: The manual details specific instances in which CMPs may be assessed.)

3 A Complete the CMP matrix for fineable violations, unsafe and unsound practices, or breach of fiduciary duties. The matrix should be prepared whenever an examiner is considering a penalty. The interagency statement of policy sets forth thirteen factors to consider when determining whether civil money penalties should be imposed:

- 3 A1 1. Evidence that the violation or pattern of violations was intentional or committed with a disregard of the law or the consequences to the institution.
2. The frequency or recurrence of violations and the length of time the violation has been outstanding.
3. Continuation of violation after the respondent becomes aware of it, or its immediate cessation and correction.
4. Failure to cooperate with the agency in effecting early resolution of the problem.
5. Evidence of concealment of the violation, or its voluntary disclosure.
6. Any threat of or actual loss or other harm to the institution, including harm to public confidence in the institution, and the degree of any such harm.
7. Evidence that participants or their associates received financial or other gain, benefit, or preferential treatment as a result of or from the violation.
8. Evidence of any restitution by the participants in the violation.
9. History of prior violations, particularly where similarities exist between those and the violations under consideration.
10. Previous criticism of the institution for similar violations.
11. Presence or absence of a compliance program and its effectiveness.
12. Tendency to create unsafe or unsound banking practices or breach of fiduciary duty.
13. The existence of agreements, commitments, or orders intended to prevent the subject violation.

- 4 CMP recommendation should only be considered if it meets the test of gravity after considering the above 13 points and when any one of the following criteria is present:

- 4 A The bank suffers a substantial financial loss as a result of the violation.
- 4 B The violation is willful, flagrant, or otherwise evidences bad faith on the part of the bank or individual involved in the violation.
- 4 C An insider (or associate) directly or indirectly involved in the violation materially benefited from the transaction.

- 4 D Previous supervisory means have not been effective in eliminating or deterring violations.
- 5 If the examiner decides to recommend CMPs, the following procedures should be implemented:
 - 5 A Consult with the Regional Office to determine the documentation necessary to support the violation and the CMP recommendation.
 - 5 B Prepare a memorandum to the appropriate Regional Director addressing the 13 points and specifying the recommendation.
 - 5 C Include the home mailing addresses for all directors and any other individuals involved in a fineable violation in the confidential pages.
 - 5 D Discuss the violations with management, but, if necessary to discuss CMPs, limit discussions to the criteria used to determine whether to assess a penalty.
 - 5 E Examiners should not discuss penalties regarding Section 8 matters. If questioned, discussions should be limited to stating that CMPs can be assessed for noncompliance with an order. (Note: Only the Regional Director can determine compliance with a Section 8 Order.)
 - 5 F If the violation involves financial gain to an insider or financial loss to the bank, examiners should attempt to quantify the amount of loss. The violation write-up should include the monetary amount and method of calculation. If the amount can not be determined, the examiner should include the reason why.
 - 5 G Copy evidence supporting the violations and retain in field office files in a separate labeled folder apart from the regular workpapers.

SUSPICIOUS ACTIVITY REPORTS

- 6 Notify the appropriate bank regulatory officials of suspected activities and actions taken.
- 7 Discuss the possibility of administrative and enforcement actions with executive management and the board of directors. If suspicious activity is discovered, and the Reserve Bank or Regional Office concurs, examiners should report the discovery of the suspicious activity and any related apparent violations to the bank's board of directors.
 - 7 A Examiners should present the facts giving rise to the apparent violation, but avoid any conclusions as to guilt or innocence of any particular individuals.
 - 7 B Remind the board of the regulatory requirements to report apparent violations promptly to law enforcement agencies and the appropriate supervisory officials. (FDIC: Regional Director.)
- 8 Determine if management has or will file Suspicious Activity Reports (SARs). (Note: Examiners should generally bring apparent criminal activities to management's attention for reporting by the bank. Under certain situations, it may not be appropriate to notify bank officials.)
- 9 Prepare SAR if the report submitted by the bank is deemed inadequate or the suspected criminal conduct has not been reported by the bank, and the examiner believes it is in the best interest of the agency. (FDIC: Refer to RD memo 96-027 for guidance on preparing and submitting SARs to the interagency SAR system. An SAR prepared and entered into the SAR system by the bank does not prevent examiners from making a more detailed report. SARs should be completed when the

Impact Analysis

examiner first obtains evidence to support a belief that a crime has been committed. Do not wait until the examination concludes.)

10 If the examiner is preparing the SAR, use the appropriate software.

10 A Attach copies of documents that prove or support the suspected criminal violations.

10 B Segregate and store additional supporting documents.

11 If authorized by the appropriate supervisory official, the examiner may communicate the details of a criminal referral directly to the FBI or the US Attorney's office.