MANAGEMENT AND INTERNAL CONTROL EVALUATION

Components of Internal Control

Overall Assessment: Does the examination analysis and review indicate that risks are appropriately identified, measured, monitored, and controlled?

C.1.	**Has management established an adequate control environment throughout the organization?**
C.2.	**Are the major risks that influence the success or failure of the bank identified and assessed?**
C.3.	**Are adequate control activities in place to ensure adherence to bank policies, and legal and regulatory requirements?**
C.4.	**Are effective information and communication systems in place to enable personnel to carry out their duties?**
C.5.	**Are appropriate systems, including audits, in place to monitor the activities of the bank?**

MANAGEMENT AND INTERNAL CONTROL EVALUATION

Specific Review Procedures

Control Environment

1. **Determine if management has taken appropriate actions to comply with Guidelines for Establishing Standards for Safety and Soundness.**

Comments:

2. **Determine if management takes adequate and timely corrective action to address recommendations by auditors and regulatory authorities.**

Comments:

3. **Determine if the board of directors minimizes operating management's ability to override policies and procedures through effective monitoring and enforcement of established guidelines.**

Comments:

4. **Determine the appropriateness of salary levels and compensation arrangements for executive management. Review the following areas:**

   - **Board approval of personnel compensation including individual salaries and benefits;**
   - **Bank purchases of life insurance;**
   - **Golden parachute agreements.**
   - **Incentive-based compensation; and**
   - **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.**

Comments:

5. **Determine if self-serving practices or conflicts of interest exist and if adequate systems are in place to monitor and manage these conflicts of interest.**

- **Determine if insiders have undue influence over customer activities.**
- **Determine if insiders are lending personal funds to customers or borrowers.**
- **Assess if privileges or benefits given to insiders are commensurate with the services rendered.**
- **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.**
- **Determine the appropriateness of any transactions related to insiders purchasing or using bank assets, such as ORE, repossessed vehicles, excess equipment, and bank facilities.**

Comments:

6. **Determine if the board of directors appropriately monitors and manages conflicts of interest between the institution and its directors, management, principal shareholders and affiliates (collectively, "associated persons"), including conflicts arising from transactions between the institution and an associated person. The board of directors should ensure the institution has policies and standards designed to ensure that:**

- **All transactions between the institution and an associated person are sound, in the best interest of the institution, and appropriately documented; and**
- **Any exceptions to the institution's established policies and standards governing transactions with associated persons are legally permissible and appropriately approved and documented.**

Comments:

7. **Determine if changes in external auditors or legal counsel occurred and why.**

Comments:

Risk Assessment

8. **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.**

   - **Determine if management's risk-taking practices are conservative, moderate, or aggressive.**
   - **Determine if the controls are in place to mitigate any concerns regarding risk-taking practices.**
   - **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.**

Comments:

9. **Determine if management plans effectively. Consider the following issues:**

   - **Strategic plan, budget process, profit plan, and growth projections;**
   - **Individuals involved with the planning process;**
   - **Reasonableness of assumptions;**
   - **Method of comparing actual performance against objectives;**
   - **Frequency of revisions;**
   - **Research efforts of new strategic initiatives such as new products and investments, branch expansion, and acquisitions and mergers; and**
   - **A business continuity planning process that incorporates enterprise wide considerations.**

Comments:

10. **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:**

    A) **External sources of risk such as:**
       - **Technology changes;**
       - **Competitors' actions;**
       - **Economic conditions;**
       - **Political and regulatory conditions; and**
       - **Accounting pronouncements.**

    B) **Internal sources of risk such as:**
       - **Retention of key management and staff;**
       - **Availability of funds;**
       - **Information systems;**
       - **Corporate restructuring;**

- **Rapid growth; and**
- **New products or business lines.**

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

Comments:

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

Comments:

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

- **Effectiveness of the bank's internal operations;**
- **Amount of cash, securities, and negotiable items normally held;**
- **Number, experience, and turn-over rate of personnel;**
- **Trust activities;**
- **Merchant credit card activities;**
- **Data processing activities; and**
- **Previous fraudulent activities or claims.**

Comments:

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

Comments:

14. Determine the reasons for any significant fidelity insurance claims.

Comments:

Control Activities
15. 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. Comments:
16. 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. Comments:
17. Determine whether management maintains an effective system of controls and safeguards for activities that expose the bank to risk. Consider the following issues: • **Authorization requirements;** • **Joint custody arrangements;** • **Dual control; and** • **Separation of duties.** Comments:
18. Determine whether the bank has effective corporate business resumption and contingency planning. Consider if the bank maintains off-premise storage of back-up files for all critical records. Comments:
19. Determine if management takes appropriate steps to comply with laws and regulations. Comments:
20. Determine if management files appropriate suspicious activity reports, if necessary. Comments:

Information and Communication

21. Determine whether information systems are in place to identify, capture, and report relevant internal and external information.

- **Assess if the systems are adequate in the higher risk areas.**
- **Determine if management regularly reviews information systems for accuracy.**
- **Consider the accuracy of the Consolidated Reports of Condition and Income.**

Comments:

22. Evaluate whether communication of information is sufficient for personnel to carry out their responsibilities.

Comments:

Monitoring

23. 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:

- **Credit Risk;**
- **Market Risk;**
- **Liquidity Risk;**
- **Operational Risk;**
- **Legal Risk; and**
- **Reputation Risk.**

Comments:

Audit and Other Independent Reviews (Monitoring)

24. Determine that an Audit Committee has been established and evaluate the composition of the committee. Consider the following:

- **Number of members;**
- **Number of outside directors;**
- **Independent of management; and**
- **The presence of any "financial experts" on the committee.**

Comments:

25. Determine that the Audit Committee operates under an appropriate charter. At a minimum the charter should address the following broad topics:

- **Requirements for Audit Committee membership;**
- **Frequency of committee meetings;**
- **Responsibilities for engaging independent accountants and appointing the internal auditor;**
- **Responsibilities for reviewing internal audits, the annual external audit and the review of quarterly and annual financial statements;**
- **Requirements and responsibilities for the supervision of the internal audit program;**
- **Guidelines for establishing open avenues of communication among the audit committee, the internal auditor, the independent accountant and the board of directors; and**
- **Authorization of funding for the audit committee to obtain outside legal counsel where appropriate and provisions regarding resources and authority to conduct investigations appropriate to fulfilling its responsibilities.**

Comments:

26. Determine that Audit Committee responsibilities are commensurate with the size, activities, and risk profile of the organization. Responsibilities would generally incorporate the following macro concepts:

- **Review and approve the audit organizational structure, including the selection, termination, and compensation of external auditors and outsourced internal audit vendors when utilized. On an annual basis, the Committee should review and evaluate the independence of the external auditors as well as vendor arrangements.**

- **Retain auditors who are fully qualified to audit the kinds of activities in which the organization is engaged and have significant input into hiring senior internal audit staff, setting their compensation, and evaluating their individual performance as well as overall performance and effectiveness of the internal audit program.**

- **Establish schedules and agendas for regular meetings with internal and external auditors, review and approve annual audit plans (and changes thereto) and monitor progress in completion of audit schedule.**

- **Review the regular internal reports to management prepared by the internal auditing department and management's response.**

- **Monitor, track, and when necessary, provide discipline to ensure effective and timely response by management to correct control weaknesses and violations of laws and regulations identified in internal and external audit reports as well as examination reports.**

- **Foster forthright communications and establish and maintain processes in which employees of the organization are able to submit confidential and anonymous concerns to the committee about questionable accounting, internal accounting control, and auditing matters.**

- **In consultation with the independent accountants and the internal auditors, review the integrity of the organization's financial reporting processes, both internal and external.**

- **Review the organization's annual financial statements and any reports or other financial information submitted to any governmental body, or the public, including any certification, report, opinion, or review rendered by the independent accountants.**

- **Review any significant disagreement among management and the independent accountants or the internal auditing department in connection with the preparation of the financial statements.**

- **Consider the independent accountants' judgments about the quality and appropriateness of organizations accounting policies as applied in its financial reporting.**

- **Consider and approve, if appropriate, major changes to the organization's auditing and accounting principles and practices as suggested by the independent accountants, management, or the internal auditing department.**

Comments:

27. Determine that committee minutes document significant actions. Minutes should generally address the following broad topics:

- **Formal review and approval of the organizational Code of Ethics and Audit Charter;**
- **Recommendations for selection and approval of the external auditors;**
- **Discussion and validation of the CPA firms "independence";**
- **Approval of the internal auditor salary as well as overall audit department budget;**
- **Review of the annual internal audit plan and subsequent review of the status of performance;**
- **Document consideration given to internal audit staffing levels and training needs;**
- **Discussions with the CPA firm regarding the quality, not just acceptability of accounting principles;**
- **Formal review and approval of annual and quarterly financial statements prior to issuance; and**
- **Review and approval of attestation letters for internal control reports.**

Comments:

---

28. If the internal audit function, or any portion of it, is conducted by outside vendors, review and evaluate the following:

- **Whether the internal audit vendor arrangement is with the same organization that conducts the financial statement audit;**

- **The outsourcing arrangement contract and engagement letter between the organization and the vendor.**

- **Due diligence assessment of vendor competence, independence, and objectivity prior to entering the outsourcing arrangement;**

- **Effectiveness of process management between the organization and the vendor;**

- **Effectiveness of communication of findings and adequacy of reports between the organization and the vendor;**

- **Whether the scope of outsourced audit work is revised appropriately when the bank's environment, activities, risk exposures, or systems change significantly; and**

- **Contingency planning to mitigate discontinuity of audit coverage in the event that the outsourcing arrangement is terminated.**

Comments:

---

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

- **The audit department is segregated from operations in the organizational structure;**
- **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;**
- **Reporting procedures of the auditor are independent of the influence of operating personnel; and**
- **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.**

Comments:

---

30. Determine if internal audit department policies and procedures are adequate for the size, activities, complexity, and risk profile of the organization. At a minimum, audit guidelines should address the following items:

- **Audit work programs;**
- **Internal Control Questionnaires/Narratives;**
- **Risk analysis and assessments;**
- **Confirmations;**
- **Workpapers; and**
- **Reporting Standards.**

Comments:

---

31. Determine that the size of the audit staff is appropriate and that related academic backgrounds, experience, competency, and ongoing training initiatives are sufficient for the size and complexity of the bank.

Comments:

---

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:

- **All important bank functions and services are subject to audit;**
- **The audit schedule is reviewed and approved by the Audit Committee;**
- **The auditor periodically reports progress in completing the schedule to the Audit Committee;**
- **Audit plan and frequencies are reasonable and are completed as scheduled; and**
- **Starting dates and time intervals between audits are changed in order to avoid anticipation by those subject to audit.**

Comments:

33. Determine if internal audit records are adequate.

- **A reasonable record retention schedule is maintained for audit records.**
- **Audit work programs are sufficiently robust to conduct an effective audit and are updated to keep pace with industry change (new products, changes in regulation, etc.)**
- **Audit workpapers contain approval of significant deviations from audit procedures.**
- **Workpapers should be well organized and supportive of conclusions drawn.**
- **Workpapers should be cross-referenced to procedures and to bank reports and totals.**
- **Workpapers contain evidence that audit managers have reviewed the workpapers for findings and final conclusions.**
- **All significant and unresolved exceptions are noted in the workpapers and included in audit reports.**
- **Responsibility for maintaining the audit manual is assigned to appropriate staff.**

Comments:

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

- **The auditor submits formal reports to the board of directors or the appropriate committee regarding material weaknesses or other unsatisfactory matters.**
- **Audit reports should include an overall opinion on the area being audited as well as opinions regarding the effectiveness of internal controls and compliance with procedures.**
- **The board or appropriate committee supports the audit staff in resolving audit matters.**
- **Departmental managers commit to take specific actions to resolve matters noted in the audit reports.**
- **The audit reports include a summary of the effectiveness of controls in the department or function.**
- **The auditor maintains a formal record of all unresolved audit or regulatory exceptions and recommendations.**

Comments:

35. Determine the adequacy and the reliability of work performed by the internal auditors by comparing examination findings in other modules to that of internal audit findings and overall evaluation.

Comments:

36. Review the bank's external audit program.

- **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.**

- **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 judgment 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 a negative comment.**

- **Determine that the organization has not entered into external audit arrangements that include unsafe and unsound limitation of liability provisions identified in the February 9, 2006 Interagency Advisory.**

- **Determine that any issues presented in the CPA management letter have been addressed.**

- **Review any additional CPA reports and follow-up on issues presented.**

Comments: