

This section is intended to determine if the organizational structure, the resources, and the control policies and procedures are adequate to foster effective information support. It will also address the quality of management and supervision of the data processing activity, including management's administrative process. The examiner should document findings especially those that do not satisfy the recommendations outlined in the *1996 FFIEC IS Examination Handbook*. This document will be included in the workpapers.

ORGANIZATION

1. Review the corporate and Information Systems (IS) departmental organization charts to determine if:
 - a. The organizational structure provides for effective IS support throughout the organization.
 - b. IS management reports directly to senior level management.
 - c. The IS department has maintained its independence from user departments.
 - d. Appropriate segregation of duties is provided.
2. Review biographical data of key personnel and the established staff positions to determine the adequacy of:
 - a. Qualifications.
 - b. Staffing levels.
 - c. Provisions for management succession.
3. Review and evaluate written job descriptions to ensure that:
 - a. They are maintained in writing and are updated promptly.
 - b. Authority responsibility and technical skills are clearly defined.
4. Test key positions to determine if the job descriptions are reasonable and represent actual practice.

5. Review IS department personnel separation procedures for adequacy.
6. Determine if management provides an adequate orientation and continuing education programs.
7. Determine the adequacy of the compensation program and its effect on staff retention or turnover.
8. If IS employees have duties in other departments , determine if:
 - a. Management is aware of the potential conflicts such duties may cause.
 - b. Conflicting duties are subject to appropriate supervision.

PLANNING

9. Obtain or prepare a list of board, IS steering, or relevant management committees that meet regularly to review IS related matters. Indicate the title of each member and determine if IS group, user community, and audit are well represented.
10. Review the minutes of the board of directors and relevant committee meetings for evidence of senior management support and supervision of the IS activities.
11. Determine if committees review , approve, and report to the board of directors on:
 - a. Short-, and long-term IS.
 - b. IS operating standards, including computer security and data security standards and procedures.
 - c. Resource allocation (e.g., major hardware/software acquisition and project priorities).
 - d. Status of major projects.
 - e. IS budgets and current operating cost.
 - f. Research and development studies.

- g. Corrective actions on significant audit deficiencies.
12. Determine if the board of directors or senior management gives adequate consideration to the following IS matters when formulating the institution's overall business strategy:
- a. Is strategic plans.
 - b. Current status of the major projects in process or planned.
 - c. Staffing levels.
 - d. IS operating costs.
 - e. IS contingency planning.
 - e. Institution business recovery planning.
13. Review the strategic plans for is activities. Determine if the goals and objectives are consistent with the institution's overall business strategy. Document significant changes recently made or planned that affect the institution's organizational structure, hardware/software configuration, and overall data processing goals.

CONTROL

14. Determine if IS management has adequate standards and procedures governing:
- a. Personnel administration.
 - b. Systems development and support functions.
 - c. Computer operations.
 - d. Telecommunications network operations.
 - f. Computer and information security.
 - g. Contingency planning/disaster recovery.
15. Determine if the standards and procedures outlined in step 14 address:

- a. Adequate segregation of duties.
 - b. Limiting access to sensitive information system resources (e.g., magnetic media, documentation, and computer equipment).
 - c. Ensuring authorization of all activities within the IS area.
 - d. Creating sufficient audit trails that would allow independent verification by the user groups.
16. Determine the effectiveness of the reports used by senior management or relevant management committees to supervise and monitor the following IS activities:
- a. Management reports that provide the current status of software development/maintenance activities.
 - b. Performance and problem reports prepared by user groups.
 - c. System use and planning reports prepared by operating managers.
 - d. Internal and external audit report of IS activities.
17. From management reports, measure actual performance of selected major projects against established plans. Determine the reasons for the shortfalls, if any.
18. Determine if management has taken positive action toward correcting exceptions reported in audit and examination reports.

FINANCIAL ANALYSIS

19. Analyze financial statements and IS operating costs to determine:
- a. Cost allocation method.
 - b. That cost allocation methods applied are similar for both affiliated and non-affiliated customers.
 - c. The significance of IS revenues from non-affiliated users relative to the institution's overall financial condition.

- d. If fees charged affiliated customers are reasonable.
 - e. If the institution has a contingency plan to provide for the loss of revenues from the non-affiliated sources, where significant, through competition or technological changes.
20. If the servicer is not a financial institution, list:
- a. Ownership, naming owners of 5 percent or more of the stock.
 - b. The members of the board of directors, indicating:
 - Name.
 - Occupation.
 - Principal business affiliation.
 - Relationship with other affiliates of this institution, if applicable.
21. If the institution receives significant outside data processing support, as identified in step 5 of the Examination Planning section:
- a. Provide the name and location of the servicers. Include any known affiliations with financial institutions or its vendors.
 - b. Determine that the services are covered by a formal written service agreement.
 - c. Determine if the agreement is directly with the servicer or through a third party. Identify the third party, if applicable.
 - d. Determine if the institution has reviewed the current financial condition of its IS servicer.
 - e. Determine that management has requested from its regulator information on the most recent examination of its service(s).
22. Based on the information available, determine if any servicer raises concern, because of financial weakness or inadequate operational controls. If such concern exists:

- a. Determine if conditions have been satisfactorily resolved.
 - b. Determine what action has been taken to correct the conditions.
 - c. Determine if management has identified or secured alternative sources of IS support if conditions are not corrected within the specified time frame.
23. Review the adequacy of insurance coverage (if applicable) for:
- a. Employee fidelity.
 - b. IS equipment and facilities.
 - c. Media reconstruction.
 - d. EFTS activities.
 - e. Loss resulting from business interruptions.
 - f. Errors and omissions.
 - g. Extra expenses, including back up site expenses.
 - h. Items in transit.
 - i. Other probable risks.

SYSTEMS CONVERSIONS

24. Review the systems conversion, controls associated with its implementation, and implementation progress achieved relative to conversion target date and:
- a. Project management records.
 - b. Minutes of conversion team meetings.
 - c. Internal and external correspondence pertaining to the conversion.
 - d. File conversion balancing procedures and results of file conversion tests.
 - e. Evidence of successful completion, as applicable, of product mapping, data mapping,

system user options selection, user acceptance testing, user procedures, and user training.

- f. Proof of successful testing of network connectivity to the new vendor's facilities and adequate progress in implementing new vendor-related disaster recovery plan and information access controls.

CONCLUSIONS

- 25. Review the results of work performed in this section and in sections for Planning and Audit. If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.
- 26. Summarize the strength and weakness of the condition of IS activities in this area.
- 27. Discuss with management:
 - a. Violations of law, rulings, regulations, or significant internal control deficiencies.
 - b. Recommended corrective action for deficiencies cited.
 - c. Management's proposed actions for correcting deficiencies.
- 28. Assign rating (see Chapter 5 for additional information).
- 29. Provide any additional information that will facilitate future examinations.

Examiner | Date

Reviewer's Initials