

IS SERVICING – PROVIDER AND RECEIVER (FILE NAME ON DISK # 2 = S2C22.WPD)

CHAPTER 22

Information Systems (IS) servicing can be viewed from the perspective, of the service provider or the receiver. Many control and administration issues are common to both. Although control issues are usually discussed from the viewpoint of the service provider, most are also pertinent to the service receiver. Separate workprograms have been provided in this chapter to aid examiners in reviewing servicing activities from the two distinct perspectives.

IS controls are important in the customer servicing and user control areas. Controls similar to those in other information processing areas should be used in customer servicing and user operations to maintain information integrity. This is particularly important when IS servicing is performed off-site.

The interchange of services between organizations entails certain risks and responsibilities that must be addressed by both the servicer and the user. Some of these can be defined and delegated within a service contract; others must be handled by each party through implementing proper operational controls.

This section describes operational and technological controls, guidelines for insurance coverage, and servicing contracts. Also discussed are adverse servicing contracts and improper financial inducements to insured financial institutions. This chapter addresses the responsibility to obtain and analyze adequate financial information from the servicer and/or client. Financial institutions depend increasingly upon servicers to provide information processing. The most difficult operational calamity for a financial institution to provide for is the termination of processing services from the servicer's bankruptcy. This chapter discusses issues specifically affecting service providers and examination objectives for reviews of service receivers.

Under provisions of the Bank Service Corporation Act, Sec. 1867, when a financial institution contracts for information processing services, it must notify its

primary regulatory agency of this service relationship. The institution should notify its agency within 30 days after signing a contract or the commencement of services, whichever occurs first.

USER INSTITUTION CONTROLS

When IS services are provided by an external servicer, many of the financial institution's operational controls should be extended to encompass the servicer. Using computerized programs and networks, financial institution employees maintain millions of accounts and record similarly high numbers of transactions every day. Text processing systems store vast amounts of correspondence. Financial institutions routinely transfer their own and customer funds ranging in the billions via computerized systems.

Transmission of data and funds regularly occurs over public communications links, such as telephone lines and via satellite. The use of new technologies to transfer funds and records, while improving customer service and institutions' internal operations, also has increased the chances of errors and abuses, such as loss of funds, loss of competitive advantage, lawsuits arising from damaged reputations, improper disclosure of information, and regulatory sanctions.

Controls must be created to minimize the vulnerability of all information and to keep funds secure. Management must assess the level of control against the degree of exposure and the impact of unexpected losses on the institution. Various ways are available to strengthen information and financial security in financial institutions. The most basic are sound policies, practices, or procedures, including physical security, separation of duties, internal quality control, hardware and software access controls, and audits.

Management should institute information security controls to:

- Ensure the integrity and accuracy of management information systems.
- Prevent unauthorized alteration during data creation, transfer, and storage.
- Maintain confidentiality.
- Restrict physical access.
- Authenticate user access.
- Verify accuracy of processing during input and output.
- Maintain backup and recovery capability.
- Provide environmental protection against damage or destruction of information.

Although they vary, security features usually are available at each level of computer sophistication. Regardless of the controls adopted, they should apply to information produced and stored by both automated and manual methods.

In many cases, financial institutions have chosen to establish and communicate security principles in writing. If sound principles are not effectively practiced, the regulatory agency may require management to establish written policies to formally communicate risk parameters and controls.

Examiners may periodically conduct reviews of information security. These reviews may include:

- The adequacy of security practices.
- Compliance with security standards.
- Management supervision of information security activities.

Manual Controls

The following discussion briefly covers basic operational controls that should be in place in a serviced institution environment. Similar controls also apply to work processed by a separate IS department within the user's own institution.

Separation of Duties

A basic control used in any internal control system is separation of duties. With this control in place, there must be collusion for any improper activities to occur. Therefore, no one person should be able to initially authorize and execute a complete transaction. Servicer personnel should not initiate transactions or correct data except when such activity is required to complete processing in a reasonable time period. If this unusual situation arises, transactions should be approved by appropriate levels of management at the information processing center and at the serviced institution. Documented approvals, with details of the circumstances that required this action, should be maintained at the processing center and the serviced institution.

Input and output duties normally should not be performed by the same person. In some instances, staff limitations may cause one person to be responsible for several activities. Included among these concentrated activities are:

- Preparing data for input to the system or shipment to the external servicer.
- Performing data entry functions, including operating check reader/sorter machines, proof machines or data conversion devices such as optical scanners or other imaging equipment.
- Preparing rejects for reentry into the system; reconciling output to input or balancing the system.
- Distributing output to ultimate users.
- Posting the general ledger and balancing computer output to the general ledger.

Internal control may be improved through rotation of assignments and scheduled, periodic absences. This will help prevent one person from having total control over any one job for an extended time period and will provide cross-training and personnel backup. These absences are most effective if they extend over the end of an accounting period or for two or more consecutive weeks.

Written policies and procedures, when used as training and reference documents, may help facilitate job rotation. Application manuals usually consist of a user's guide provided by the servicer and supplemented by procedures written by the user. Manuals normally cover preparation and control of source documents, and certain control practices pertaining to moving documents or electronic images to and from the user and servicer, the daily reconciliation of totals to general ledger, and changes to master files.

Dual control should be used in automated systems. Supervisory holds should be placed on customer accounts that require special attention. Certain types of transactions, e.g., master file changes, should require special transaction codes before the activity can be completed. When account information is added/removed or when a transaction requiring supervisory approval is completed, exception reports will be printed and should be promptly reviewed by a designated person not involved with the original transaction. In general, automated dual control methods are superior to manual procedures. Many current financial software applications use automated balance and control features. Presentations to the users are performed on-line rather than using a manual comparison of hardcopy reports to source documents.

Internal Quality Controls

Internal controls fall into three general categories: administrative, dollar, and nondollar.

Administrative controls usually result from management review of daily operations and output reports. Each application includes basic controls and exception reports that are common to all financial institution operations. To be effective, exception reports and controls must be properly used, especially methods for controlling dormant accounts, kiting, drawings against uncollected funds, overdrafts and posting computer-generated income and expense entries.

Dollar controls ensure processing for all authorized transactions. Balancing procedures should be complete and trial balances must be reconciled to original source input and to the general ledger. Report distribution should follow a formal procedure.

All rejects must be accounted for, corrected and resubmitted, and all exception reports should receive proper supervisory attention.

Nondollar control totals are used when dollar values are not present, as in name and address changes. Controls should be established before processing this work and be properly reviewed to ensure that all nondollar transactions are being processed. For example, new account reports should be checked against new account input forms or written customer account applications to assure that data has been properly entered. To protect data integrity, procedures should be developed to control master file and program changes. The serviced institution should verify that only its authorized changes are used to alter information, and that the processing center employees do not initiate master file changes.

TECHNOLOGY CONTROLS

Data Communications

Data communications system controls should be reviewed by the serviced financial institution. The controls available to the user can be generally categorized into: user identification, levels of accessibility, restricted transactions, and activity and exception reports.

User Identification

This control allows only authorized personnel to use the system and requires personal and workstation identification for each transaction entered. Users may be identified by key, token, password and/or identification number (IDs). When workstations are equipped with key, card-type locks, or tokens, strict control of access devices is necessary to protect the computer system. Many systems use software controls which require passwords and/or IDs to gain access to the system. Security procedures should strictly control access to those user IDs, and passwords/numbers should be changed regularly. Some workstations can be controlled by restricting access to the work area by placing them in a remote or locked area, or by establishing definite times for remote activity via system invoked time-of-day controls. Servicers may offer these features as standard access control elements, but actual information security practices could vary widely at

the serviced institution level. Therefore, it remains important to determine that these controls are implemented properly by the serviced institution.

When a workstation is not hardwired or permanently connected to a host computer, special manual and automated controls must be established to ensure proper host/terminal relationships. Automated dial-back procedures may be used, where the computer calls the PC back to authenticate access. Other automated methods may include software checks on hardwired terminal ID numbers, or a dialogue between the data communications software and workstation or PC.

Level of Accessibility

Another basic control is to allow each user to access only that information needed for that person's duties. One person should not be able to make all transactions relating to a given event. For example, when a loan is charged-off, one person should not control adjustments to both the loan and general ledger applications without appropriate compensating controls. In those systems where the general ledger entries are auto-posted, another staff member should review the general ledger entries promptly.

An automatic timeout feature provides a benefit with minimal processing risk. Since the unattended workstation can be a target for unauthorized use, this feature guards against this by automatically signing-off a user from a workstation where there has been no activity for a certain period of time. There is little user inconvenience in this feature, since to restart, the user need only reenter a password. Using time-of-day restrictions can limit unauthorized use of workstations during periods when the entire department or section would be unattended.

Restricted Transactions

Restricted transactions are specialized transactions used only by supervisory or management personnel. Examples are reversing transactions, dollar adjustments to customer accounts, or daily balancing transactions. Management should review periodically user needs and the appropriateness of restricting access to these transactions.

Activity and Exception Reports

Report output will vary depending on the sophistication of data communications and applications software. At a minimum, reports should be generated that detail transactions by workstation, operator and type. More sophisticated software will produce such reports as the number of inquiries by workstation, unsuccessful attempts to access the system, unauthorized use of restricted information, and any unusual activity, Eg., infrequently used transactions.

Activity reports monitor system usage and should be reviewed periodically by management. Exception reports should be produced and reviewed daily by designated personnel who have no conflicting responsibilities. A problem with many logging systems is that every event is recorded in the log and therefore identifying problem areas is, in many instances, cumbersome and difficult. Some operating system vendors or third-party software companies can provide software that produces more meaningful analysis and reporting from these logging systems.

Systems Features and Controls

As a communications system becomes more sophisticated, the controls also will become more complex. Generally, communication systems fall into basic levels: inquiry only, memo-post, and on-line post. However, a number of combinations and variations of these levels of systems exist and are described as follows:

- *Inquiry-only system.* This system gives the user the ability to search and review machine-readable records, but not to alter them. The number of controls and security concerns related to this system are few. A major concern is the access to confidential information.
- *Memo-post system.* This level is more sophisticated than the inquiry-only system and allows the user to create interim records. Permanent posting is done by the servicer through batch processing. Memo-post systems should be controlled by limiting physical and logical access to the system and restricting certain transactions to supervisory personnel only.

- *On-line post system.* This system, sometimes called a real-time system, requires the strictest controls because all accepted transactions entered through the communications system are permanently applied to the machine-readable records. Besides controlling access, the reports produced by the system should provide all activity and exception information and should be reviewed by appropriate levels of management.

Backup Considerations

Data communications systems are susceptible to software, hardware, and transmission problems that may make them unusable for extended periods of time. If the financial institution depends on its data communication system for its daily operations, appropriate backup provisions are necessary. Backup is the ability to continue processing applications in the event the data communication system fails. Backup can be provided in a number of ways, including via a batch processing system or PCs operating in an off-line mode, data capture at the controller if transmission lines are lost, redundant data communication lines, backup modems, or rerouted circuits from the local telephone carrier.

Regardless of the method used, a comprehensive backup plan with detailed procedures is required. Detailed procedures on how to obtain and use personnel and equipment must be included in the plan. Because of the critical nature of some on-line systems, a batch backup may not remain a viable option. Periodic tests of backup capabilities should be performed to ensure that protection is available and that employees are familiar with the plan.

Other Operational Controls

Audit

The reliability of the audit review of work processed by the servicer must be determined. Therefore, the audit review should consider the following factors:

- The practicality of the serviced institution having an internal auditor and if so, the auditor's level of training and experience.

- The training and background of the serviced institution's external auditors.
- Audit functions performed by the institution's outside auditors, by the servicer, by the servicer's outside auditor and by supervisory personnel.
- Internal IS audit techniques currently followed.

The audit should review controls and operating procedures that help protect the institution from losses due to irregularities and willful manipulations. Thus, a regular, comprehensive audit is necessary.

CPA audit reports generated on external IS servicers typically recite certain internal control measures that client institutions are responsible for, and that they must have in place in order for the servicer's accounting systems to be effective. These client institution internal control measures are essential. Financial institution management and their audit personnel should verify that the recommended institution internal controls are working effectively at their own organization, and that they effectively complement the accounting system controls described in the servicer's third-party review (See Chapter 1 for additional information on types of external audit reports and their scope).

Because of the need for an effective internal control network at the serviced institution, around-the-computer audit techniques should be performed periodically by designated personnel:

- Developing data controls (proof totals, batch totals, document counts, number of accounts, and pre-numbered documents) at the institution before submission to the servicer. The auditor should sample the controls periodically to ensure their accuracy.
- Spot-checking reconciliation procedures to ensure output totals agree with input totals, less any rejects.
- Sampling rejected, un-postable, holdover, and suspense items to determine why they are unprocessable and how they are disposed of (to assure they are properly corrected and reentered).

-
- on a timely basis).
 - Verifying selected master file information (such as service charge codes), reviewing exception reports and cross-checking loan extensions and deposit account entries to source documents.
 - Spot-checking computer calculations, such as loan rebates, interest on deposits, late charges, service charges, and past-due loans.
 - Tracing transactions to final disposition to ensure there are adequate audit trails.
 - Reviewing source input to ensure that sensitive master file change requests have the required supervisory approval.
 - Visiting the servicer periodically to assess the status of controls.
 - Examining other audits of the servicer.

In addition, through-the-computer audit techniques allow the auditor to use the computer to check processing steps. There are audit software programs to test extensions and footings, and to prepare direct verification statements. These audit software programs often can invoke statistical sampling routines in generating their audit confirmations. If a serviced institution has audit software, provisions should be made with the servicer to allow its use.

Regardless of whether the information processing is done internally or through an outside servicer, the financial institution's board of directors must provide an adequate audit program for all information systems. If the institution has no internal IS audit expertise, the nontechnical audit methods can provide minimum coverage. This should be supplemented by comprehensive outside IS audits (See Chapter 1 for additional information on types of external audits, their reports, and their scope).

INSURANCE FOR USER INSTITUTIONS AND SERVICER PROVIDERS

A financial institution should review its internal operations, the transmission or transportation of automated records or data, and the type of processing being performed at the servicer. This review should identify the risks and accountability at both, the user and servicer locations, and while in transit. The

institution should review the available insurance coverage to determine what coverage should be obtained by the institution (See Chapter 9: Management for additional information on insurance coverage). Insurance covering physical disasters, such as fire and natural disasters, should be sufficient to cover replacement of the computer system. Coverage that protects specialized computer and communications equipment may be more desirable than that provided by regular hazard insurance. Expanded coverage provides protection against water infiltration, mechanical breakdown, electrical disturbances, excessive changes in temperature, corrosion, etc. The use of an agreed-amount endorsement can provide full recovery of covered loss.

Coverage in effect at the servicer should be reviewed to determine if its amounts and types are adequate and that it is the same as the financial institution would purchase if the processing was done internally. Coverage provided by the servicer should complement and supplement the institution's coverage. Where servicer coverage is not sufficient, the user institution should consider obtaining coverage. Additionally, if the loss is under the user's coverage, it need only prove that a loss occurred to make a claim. If the loss is under the servicer's coverage, the institution must prove that it occurred and was caused by the servicer, in order to make a claim. The serviced institution's blanket bond coverage should be reviewed, as well as, similar coverage provided by the servicer. Standard Form 24 fidelity coverage (also called the Financial Institution Bond) provides the institution with broad risk coverage.

The coverage period is stated in terms of a fixed time period. The loss, the discovery, and the reporting of the loss to the insurer must occur during that stated period. Extended discovery periods are available generally at additional cost if the bond is not renewed. The dollar amount of the coverage now represents an aggregate for the stated period. Each claim paid, including the loss, court costs, and legal fees, reduces the outstanding amount of coverage, and recoveries do not reinstate previous levels of coverage. The serviced institution's board of directors should be involved in determining insurance coverage, because each board member will acknowledge the terms, conditions, fees, riders,

exclusions, etc., of the policy. The institution must report to the insurer any existing regulatory examination findings, memorandum of understanding, cease and desist order, etc. Information provided to the insurer is considered a warranty of coverage. Any omission of substantive information could result in coverage being voided.

The institution or servicer should consider additional coverage for:

- Media reconstruction to recover the data contained on the magnetic media.
- Media replacement to replace blank media.
- Extra expense to provide reimbursement of expenses incurred over the normal cost of operations.
- Business interruption and errors and omissions coverage by the servicer.
- Transit coverage for physical shipment of source documents.
- EFTS liability coverage for operations which use electronic transmission.
- Computer systems rider to the financial institution bond which provides coverage for employee dishonesty involving the institution's computer and wire transfer systems.
- Computer crime policy which provides broader coverage than the computers systems rider, and when sold with the financial institution bond, replaces the computer systems rider. The computer crime policy affords protection against both internal and external perpetrators of computer crime and damage done by computer viruses and hackers.

The determination of purchase insurance coverage or to self insure is based on several factors: The cost of coverage versus the probability of occurrence of a loss; the cost of coverage versus the size of the loss of each occurrence; and the cost of coverage versus the cost of correcting a situation which could result in a loss. In order to evaluate these risks and the costs of insuring against these risks, some institutions engage

risk consultants. In situations where the risks are complex or the expertise of management is limited, the analysis of the proper types and amounts of insurance protection needed may best be performed by outside experts. Certain criteria should be used when using a consultant for this review: The consultant should not be affiliated with an insurance company; should not currently be underwriting or selling insurance to the financial institution; and should have a good reputation in the marketplace.

RECORD PROTECTION AND RETENTION FOR USER INSTITUTIONS

The ability of any financial institution's IS operations, whether performed internally or by an outside servicer, to survive a disaster, depends on the retention of sufficient backup data to reconstruct the institution's important records and sufficient backup capacity to process them.

When the institution is serviced, records are controlled by both the servicer and the institution. In order to provide sufficient coverage, a determination should be made as to which records are best protected at the servicer and which are best protected by the institution. The servicer's responsibility for records it stores for the institution should be detailed in the service contract. If the servicer does not, or will not, permit specific reference to record retention in the contract, then a general reference may be sufficient if closely reviewed by the institution. The institution should obtain a copy of the servicer's backup agreement and retention procedures and thoroughly understand what records are protected and to what extent. The institution should keep on file the servicer's procedures and review them periodically.

In addition to records retention procedures, the institution should review the servicer's hardware and software backup arrangements. The review should encompass the frequency of data and software backups, the location of the off-site storage facility and the materials stored at that site, the availability of software replacement or vendor support, and the amount and location of duplicate software documentation.

The servicer's hardware backup arrangements should be reviewed to determine: (1) if a commercial

recovery service is used and the amount and type of backup capacity provided under the contract; (2) if the servicer uses an alternate data center, and if the center has sufficient capacity and time to allow continued full service; or (3) if multiple processing sites within the same facility are available for non-disaster processing problems, and whether each site has an alternate or uninterruptible power supply. Arrangements at an alternate site should be able to provide adequate communications, continued transmission of data, and preparation of reports.

Some servicers do not automatically provide recovery services in normal processing agreements. Management must be sure they are covered for recovery services. Examiners should determine if a recovery service has been subscribed to or another means of operational recovery is present.

FFIEC Supervisory Policy SP-5 in Chapter 25 requires each serviced institution to evaluate the adequacy of its servicer's contingency plans. Also, it must ensure its contingency plan is compatible with the servicer.

Retention schedules for automated records are generally determined on a case-by-case basis, since the amount and type of record duplication varies from site to site. The only way to provide sufficient protection of records is to continually review the flow of documents, data and reports, and to retain the necessary records for a certain time period until more current data is available to replace it. Some records may be available in both hard copy and machine-readable formats, with the latter being the preferred format.

Hard copy, while not preferred, is often the only record available due to cost or processing considerations. In addition to the types of records being backed up, the number of existing generations of particular information and the ability to recreate current versions from older versions should be considered. Certain records have use beyond the need for reconstruction of current records. After retention for backup needs, month-end, quarter-end, and year-end files can be further used to meet reporting requirements of the institution or regulatory authorities.

Another factor to consider regarding record retention is the location of the information processing center.

If the center is located in an adjacent building, the possibility of a disaster occurring to both organizations simultaneously increases. This situation may necessitate that additional record protection procedures be instituted by the servicer or the financial institution. In this case, the importance of both parties' off-site backup materials is increased.

If a major disaster occurs, computer facilities may not be available, even if the servicer has duplicated the records on machine-readable media. Therefore, an alternate form of remote record storage that can be manually processed should be considered. Scanning or microfilming all items before being sent to the processor would protect the serviced institution should any items be lost, misplaced, or destroyed. Optical disk storage offers a viable alternative for mass data storage and retrieval after processing has occurred.

A number of records storage firms offer remote storage at a reasonable cost. Such firms can assist in developing a comprehensive microfilm or optical disk-based record protection program. User management, on the other hand, may wish to develop its own plan.

When internal processing is used, all of the information protection measures are developed and implemented by the institution. In servicing arrangements, the institution depends upon a second party to perform these activities. Whether the institution processes its own data or uses an outside servicer, it is crucial that the financial institution develop and implement a workable disaster plan.

See Chapter 13: Operations, Chapter 15: Network - Client/Server, and Chapter 16: End User Computing for additional information on alternate backup arrangements and record protection.

CONTRACTS

A poorly written or inadequately reviewed contract can be troublesome for both the serviced financial institution and the servicer. To avoid or minimize problems in such a contractual arrangement, legal counsel familiar with the terminology and specific requirements of a data processing contract should review it to protect the institution's interests. This may require hiring a knowledgeable outside attorney. Since the contract sets the terms of a multi-year

understanding between the parties, all items agreed upon during negotiations must be included in the final signed contract. Verbal agreements are not enforceable, and the inclusion of wording in the contract to the effect that no oral representations apply may protect both parties from future misunderstandings.

The contract should establish baseline performance standards for information processing services. In addition, the contract should define each party's responsibilities and liabilities, where possible.

Contracts between financial institutions and external information processing companies do not have a standard form, but rather they share a number of common elements. The contract should be viewed in its entirety, and evaluated in light of the substance and impact of its meaning, as well as the technical rights, obligations, and relief contained in it.

Minimum necessary contract elements and considerations are as follows:

1. A description of the work to be performed by the servicer.
 - Applications to be processed and services to be provided should be enumerated in, or as an appendix, to the contract.
 - The contract should contain provisions which define the responsibilities of both parties regarding the addition of future applications or the deletion of current applications. The parties' abilities and rights in modifying services performed under the contract should be fully detailed.
 - Processing frequency and report generation should be addressed. Master files updating and the holiday and weekend schedule should be specifically addressed.
2. The basis of costs, including development, conversion and processing, and additional charges for special requests.
 - Monthly processing fees should be fully enumerated. Additional charges and free

services discussed in negotiations must be incorporated into the fee schedule. And, the basis of fee calculations should be disclosed.

- If special software is developed for the institution to process its applications, ownership of these programs should be addressed. Generally, the developer of the software owns the product and can therefore sell or license it to other organizations.
 - The cost of converting the institution's records should be specified. In some circumstances, a portion of this cost is included in the monthly processing fees. If this is done, the servicer will want a contract term long enough to recapture conversion costs. In other situations, conversion costs are absorbed by the servicer. In most arrangements, negotiated costs of conversion are paid outright by the institution.
 - The time frame for conversion should be well defined so the institution can prepare its staff and facilities.
 - Costs for satisfying special management requests, audit needs, and regulatory requirements should be included in the contract.
3. Concerns regarding on-line communications availability, transmission line security, and alternate data entry.
 - Operating hours for the on-line communication network should be specified. Cut-off times for item capture and file maintenance entries should be included in the contract. If physical shipment of items to the servicer is performed, the cut-off time for inclusion in the current day's processing should be addressed, as well as the time frame for delivering reports to the serviced institution.
 - Responsibilities for security of the communications network should be addressed. Security software is now a common on-line control, and should be evaluated when choosing servicers. In many cases, message authentication can be used. This method provides certain benefits: Messages garbled during transmission may have sufficient data

for reconstruction; coverage is host-to-host so that all parts of the network are covered; and, while the messages are not private, message alteration can be determined. It also is possible to provide maximum security through a combination of these methods; however, this generally would be reserved for critical, large-dollar funds transfer areas.

4. Audit responsibility and the right of user representatives to perform audit procedures.

- The contract should identify: Whether the servicer will contract for and provide copies (to the user) of a third-party CPA review, and at what cost (if any); the timing, frequency, and type of external audit coverage that the servicer will contract for; whether the servicer will maintain an internal audit function; whether the serviced institution, alone or with other serviced institutions, will contract for a third-party CPA audit; also, when and under what conditions the client is allowed to conduct audits of the service center; or, whether the institution will conduct servicer audits with its own staff.

5. Backup and record protection provisions (covering equipment, program and data files) to ensure timely processing by the service center in emergencies.

- Contract terms should address the servicer's backup arrangements. Areas to be covered include all or a portion of the following. For on-line systems, it should be noted whether redundant files are maintained at the servicer or at a remote location and whether alternate telecommunication or processing facilities are available. For batch systems, it should be noted whether: alternate methods of transporting or rerouting document flows are available; off-site data files are maintained; or alternate computer processing sites are available. The servicer's software should be backed up, along with all necessary documentation. If the software is under a third-party escrow agreement, such arrangements should be detailed.
- Backup arrangements should be addressed as part of the agreement. Contract terms may state only that adequate backup is maintained

by the servicer, with specifics included in an appendix.

- The servicer must have an effective disaster recovery/contingency plan. The serviced institution should receive a copy of the plan. A detailed description of the disaster recovery plan test results should be provided annually by the servicer to the financial institutions. Areas where protection of the serviced institution's records are not well defined should be clarified in the contract.

6. Establishment of liability for source documents while in transit to and from the service center. If the service center is responsible, the servicer should have adequate insurance coverage for such liabilities. Maintenance of adequate insurance for fidelity, fire, liability, and data losses from errors and omissions should be addressed.

- Insurance protection maintained by the servicer should be reviewed to determine what additional coverage should be requested of the servicer or maintained by the serviced institution. Gaps in insurance protection generally account for little savings to the institution but could potentially be responsible for large losses. The institution should consider, and dismiss if appropriate, the option of self-insuring.

7. Confidential treatment of records. The servicer should be willing to protect the institution's data from unauthorized disclosure. Information which is sensitive or could be misused should receive a higher level of protection.

8. Upon the contract's termination, ownership of computer programs and related documentation, and of master and transaction data files in their machine-readable format, and the institution's right to receive these materials, should be addressed. The specific cost of returning institution data and the time frames for their return also should be clearly described, including any transitional assistance from the servicer and its cost.

9. Price changes and costs should be included. Provisions for contract cancellation or withdrawal from the servicing arrangement by either party,

including those covering adequate notification also should be addressed.

- The servicer may be allowed to raise fees to offset normal operating cost increases during the life of the contract. At the same time, the institution has the right to expect the costs of the contracted services to remain stable. Including parameters within which costs may increase provides both parties a measure of protection. Limiting the percent of allowable increases and giving the institution the ability to terminate a contract for excessive increases without penalty is desirable. The institution's obligation to pay outstanding invoices for services provided and the amount of penalty for early termination of the contract should be stated.
 - Time frames for, and methods of notifying both parties of contract termination should be stated. If early termination is allowed, costs that the servicer had postponed for conversion or other activities should be recoverable.
 - Time frames should be long enough for the serviced institution to allow orderly conversion from the present servicer to another vendor.
 - Some service contracts contain silent renewal features which automatically renew the contract for either its original term or a given term without any explicit action of either party. Often, such silent renewal features are triggered six months to one year from the contractual expiration date of the original agreement. Financial institutions should be aware of such renewal features in service contracts.
10. Processing priorities should be detailed in the contract for both normal and emergency situations.
 11. The contract should provide notification by the service center to the institution of all systems changes that would affect procedures, reports, etc.
 12. The contract should provide that financial information be provided periodically (preferably annually) by the servicer to

serviced institutions. In large corporate organizations, where the information processing servicer activities are a small portion of the total income and expenses of the corporation, the profitability and, therefore, the continued existence of an information processing subsidiary may not be well presented in an annual report. A breakdown of the subsidiary's balance sheet and income statement should be obtained. In addition, audited financial statements are of greater benefit to the financial institution than unaudited financials.

- If the servicer charges the client for copies of periodic financial statements, this should be recited in the contract.
13. Training is an area where the institution can experience a large risk exposure. Improperly or inadequately trained employees can create situations which can be costly, in both time and money, to correct. Conversion of the institution's records should be preceded by careful planning and training. Smooth operation of the system and flexibility to handle normal operating problems require sufficient training. Abnormal or emergency situations require a higher level of training for perhaps a small group of employees. The amount, type, location and cost of training, and the number of employees to be trained should be detailed in the contract.
 14. In addition to the concern of the serviced institution to protect itself through a well-reviewed and sufficiently amended contract, regulatory authorities have a contract concern regarding actions in the event of receivership. The contract should not contain special clauses which limit the ability of a regulator to arrange an orderly and reasonable conversion of data to another servicer or vendor, or to the receiver in the event of receivership. Merger, purchase, and assumption activities are hampered by excessive conversion penalties and fees. The requirement that the assuming or purchasing institution must pay the remaining balance of all monthly fees of a long-term contract reduces the ability of the receiver to provide swift and cost-effective reestablishment of

financial services to the community.

15. Contract and penalty provisions should be reviewed for reasonableness in: Length of contract versus postponed fees and charges; length of contract versus the reduction in the cost per month; establishment of large contingent liabilities through excessive penalty fees; compensation of the servicer for loss of income versus the penalty fees; and the punitive nature of penalty fees or clauses.
16. Contracts should provide a prohibition against the assignment of the contract by either party without the other's consent.
17. In some cases, servicers unbundle certain services and sell them as optional extras. This practice allows an institution to select only needed services. Tailoring services can reduce the overall cost of information processing activities. However, this practice is not acceptable when backup and data security are considered optional. These services should be mandatory because the institution which can least afford the cost of these services is also the one that can least afford not having them.
18. Finally, negotiations between two parties sometimes include the receipt of gifts, premiums, or bonuses for signing a contract for information processing services. These practices, although used in the commercial and industrial environment, are prohibited in the financial community by rules and regulations. The practice could be interpreted as bribery of a bank official rather than as a bargaining tool.

CONTRACT INDUCEMENT CONCERNS

Some financial institutions have signed servicing contracts that contain provisions that may adversely affect the institutions. Such contract provisions may include extended terms (up to 10 years), significant increases in costs after the first few years, and/or substantial cancellation penalties.

In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition

of assets or avoiding expense recognition for current charges. Institutions experiencing earnings and capital problems seem particularly attracted to these inducements.

Examples of inducements include:

- The servicer purchasing certain assets (e.g., computer equipment or foreclosed real estate) at book value, which exceeds market value.
- The servicer providing capital by purchasing capital stock from the institution.
- The servicer providing cash bonuses to the institution once the conversion is complete.
- The servicer providing up-front cash to the institution. The servicer states that the institution acquires the right to future cost savings or profit enhancements that will accrue to the institution as a result of greater operational efficiencies. These improvements are usually without measurable benchmarks.
- The institution defers expenses for conversion costs or processing fees under the terms of the contract.

These inducements may offer a short-term benefit to the institution. However, the servicer usually recoups its costs by charging a premium for the processing services it provides. These excessive fees adversely affect an institution's financial condition over the long-term. Furthermore, the institution's accounting for such inducements may be inconsistent with generally accepted accounting principles (GAAP) and regulatory reporting requirements.

Additionally, Title II of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) states:

An (FDIC) insured depository institution may not enter into a written or oral contract with any person to provide goods, products or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety or soundness of the institution (See Chapter 24 for

additional information and the legal cite).

Accordingly, when negotiating contracts, an institution should ensure that the servicer can provide a level of service that meets the needs of the institution over the life of the contract. It also is the institution's responsibility to ensure that contracts are accounted for in accordance with GAAP. Contracting for excessive servicing fees and/or failing to properly account for such transactions is considered an unsafe and unsound practice. In entering into service agreements, institutions must ensure that accounting under such agreements reflects the substance of the transaction and not merely the form. (See Chapter 25 for additional information on FFIEC SP-6: Interagency Statement on EDP Service Contracts.)

FINANCIAL INFORMATION FOR USER INSTITUTIONS AND SERVICERS

Many financial institutions have become so dependent on outside data processing servicers that any extended interruption or termination of service would severely disrupt normal operations. Termination of services generally occurs according to the terms of the service contract. Institutions also may experience termination of contracts caused by a physical disaster, such as fire or flood, or termination caused by bankruptcy. The serviced institution must prepare differently for each type.

The majority of terminations occur according to the terms of the contract. The contract should allow either party to terminate the agreement by notifying the other party 90 to 180 days before the termination date. This gives a serviced institution the time to shift to another servicer.

Termination caused by physical disaster occurs infrequently, but it may present the institution with a more serious problem than termination by contract. If the servicer has complied with basic industry standards and maintains a proper contingency plan, disruption of services to users will ordinarily be minimal. The contingency plan must require the servicer to maintain current data files and programs at an alternative site and arrange for backup processing time with another center. At a minimum, these provisions should allow the servicer to process the most important data applications. Since equipment vendors can often

replace damaged machines within a few days, the servicer should be able to resume processing with little delay. The servicer, not the serviced institution, is responsible for the major provisions of the backup contingency plan. However, the institution must have a plan that complements the servicer's.

Termination due to the bankruptcy of the servicer is potentially the most devastating to a serviced institution. There may not be any lengthy advance notice of termination or an effective contingency plan because there may be no available servicer personnel. In this situation the serviced institution inherits the responsibility for finding an alternative processing site.

Although user institutions can ordinarily obtain data files from a bankrupt servicer with little trouble, the programs and documentation required to process those files are normally owned by the servicer and are not available to users. These programs are often the servicer's only significant assets. Therefore, a creditor of a bankrupt servicer, in an attempt to recover outstanding debts, will seek to attach those assets and further limit their availability to users. The bankruptcy court may provide remedies to the user, but only after an extended length of time to adjudicate substantive matters.

At this point, a serviced institution has two alternatives:

- Pay off the creditor and hire outside specialists to operate the center.
- Transfer data files to another servicer.

Either alternative is likely to be costly and may cause very harmful operating delays.

Therefore there is an emphasis on the great importance to financial institutions of monitoring the financial condition of their servicer(s). In order to fulfill its fiduciary responsibility, a serviced financial institution will normally determine the financial viability of its servicer(s) on an annual basis. Once the review is complete, management must report the results to the board of directors or to a designated committee. At a minimum, management's review should contain a careful analysis of the servicer's

annual financial statement. Institution management also may use other forms of information to determine a servicer's condition. For example, reports of independent auditors and reports obtainable from appropriate regulatory agencies may contain information which can be vital in determining a servicer's financial condition. Managers also can use information provided by public media, such as trade magazines, newspapers, television, etc. If it becomes known that the servicer's financial condition is unstable or deteriorating, the serviced institution should put its contingency plan into effect. Even if the servicer remains in operation, its financial problems may cause it to take drastic measures that may jeopardize the quality of its service and possibly the integrity of the data in its possession. Institutions should consider a servicer's failure to provide proper financial data as an indication of unsound operating practices.

CONSIDERATIONS FOR SERVICE RECEIVERS

Senior management should review performance of the service provider. The review should cover:

- Financial condition.
- Costs.
- Ability to meet future needs.
- Quality of service.
- Control environment at the data center.
- Emergency backup provisions.
- Insurance requirements.

Problems in any area need to be discussed and a timely resolution sought. To help with the evaluation of the servicer, management should obtain all audit and examination reports available and review them thoroughly. Then, management should document their review and actions to substantiate this due diligence.

POTENTIAL SERVICE PROVIDER ISSUES

If a financial institution provides information processing services to others, it should examine the

risks in doing so and the procedures in effect to minimize that risk. Although this subsection focuses on risks which may affect the institution providing services through a computer center, the effect on the customer institutions of obtaining information services in this matter should also be weighed. Primary considerations are:

- *Possible contingent liabilities* – The center must protect and properly process accepted work. The same controls used in processing the institution's work should be maintained when processing work for others.

A well-written service contract with properly defined duties and responsibilities will protect both the servicer and the customer. Contract considerations are covered earlier in this chapter. In all cases, contracts should be reviewed by legal counsel familiar with computer service contracts.

The service provider also incurs additional liability for ensuring adequate backup of programs and files is maintained.

Contingency planning also must be expanded to coordinate with the serviced institution. Plans for obtaining input from and providing output to the serviced institution in a disaster/recovery situation need to be developed. The provisions of the plan which could affect client institution operations should be provided to the client institution. Also, the service provider should support the client's corporate contingency planning efforts in developing recovery procedures for a disaster at the client's facilities.

- *Insurance* – Financial institutions offering information processing services should be adequately protected by fidelity and other appropriate types of insurance coverage. (Insurance is discussed elsewhere in this section and in Chapter 9, Management).
- *Investment in equipment, software, and personnel* – In some instances, financial institutions make sizeable investments in equipment, software, and personnel to support customer servicing. This practice may represent a costly diversion from the primary business of a financial institution,

especially a small institution. Additionally, rapidly changing technology can render obsolete an institution's investment in information processing assets.

- *Costs* – Often new business is generated, or old business retained, due to the availability of IS servicing for customers. The cost of providing these services should not exceed the revenues generated; however, the institution must decide whether processing services are offered to generate income or to serve other less tangible purposes.

Frequently, income received from such services may more than offset additional operating expenses. Management should establish a formal method for determining costs and setting fees. Some institutions arbitrarily set their servicing fees at a level to meet or beat competition and to attract new customers, rather than establish fees based on a formal analysis of how their IS resources are used.

Economies-of-scale can be realized in equipment, facilities, and program development costs when processing assets are used by the financial institution to service others. Software development costs can be spread over a number of institutions, allowing maintenance of such programs to be a normal function of information processing, rather than specialized customer servicing.

Financial institutions sometimes offer a tailored or specially developed application to customers. However, the service must be priced to reasonably recover the development cost either initially or as part of the monthly servicing fee.

Excess equipment capacity can become a problem if it was acquired specifically for customer servicing. Normally, additional staffing will be needed, and unless these expenses can be offset by similar income increases from customers, a significant drain on the earnings of the servicing institution can result. An IS operation consisting solely of one set of standardized applications is easier for management to control and administer.

- *Quality of service* – The quality of service offered to outside organizations is not always easy to assess. However, some complaints can be heard through discussions with the customer service

representatives or the correspondent departments. In addition, the processing center should maintain a complaint file. Any complaints received should be thoroughly investigated and resolved by the servicing institution. The quality of servicing also can be monitored by reviewing customer contract cancellations, renewal rates, and payment delinquencies.

- *Control of documents* – If the service center prepares checks or other negotiable documents, the blank stock should be adequately controlled. Facsimile signature plates should not be maintained under the sole control of persons involved with center operations.
- *Billing* – When a financial institution provides services to other financial institutions, the receipt of service center income should be handled by a department other than the IS organization. This provides better separation of duties. The computer system should accumulate activity counts and would likely generate billing. Also, cost accounting data should be maintained so that center management can decide about future application services. In a holding company environment, the appropriateness of fees charged to subsidiaries should be reviewed.
- *Audit* – The internal auditor should compare, at least annually, customer service billing against IS activity records and comparative income and activity reports. A representative number of entries should be traced from source to payment. Also, it should be determined that customer records, supporting programs and documentation are afforded the same level of security and access control as the servicer's records.

POTENTIAL SERVICE RECEIVER ISSUES

If a financial institution receives information processing services from others, it should examine the risks in doing so and the procedures in effect to minimize that risk. Management's primary considerations should be to:

- Assess the types and levels of risks associated with information systems services received.
- Assess the adequacy of the system of controls safeguarding the integrity of the data processed by

the service provider.

- Develop, implement, and test contingency plans that will ensure the continued operation of the institution's data processing tasks/needs in the event of unforeseen events. Contingency plans should address both a disaster at the service receiver's facilities and a disaster at the service provider facility.

- Implement an effective system to monitor the financial condition of key data processing servicers.
- Expanded audit function to review controls at the service provider's facility if an adequate audit is not performed via a third-party review or some other acceptable means.