

COMMUNITY FINANCIAL INSTITUTION CHAPTER 23 IS EXAMINATION PROGRAM

(FILE NAME ON DISK # 2 = S2C23.WPD)

COMMUNITY WORKPROGRAM

The Community Financial Institution IS Examination Workprogram in smaller serviced institutions helps determine if controls are adequate for evaluating and controlling IS risk when selecting a servicer, signing data processing contracts, establishing IS controls in user departments, establishing microcomputer controls, and developing and testing a disaster contingency plan. Use of either procedure ensures that IS risk is periodically evaluated in all institutions. The findings and conclusions of this program are included in the safety and soundness ROE, as appropriate.

The Community Financial Institution IS Examination Workprogram helps the examiner evaluate IS related internal control procedures in smaller financial institutions using vendor supplied and supported software. In all cases the use of the FFIEC Community Financial Institution workprogram is predicated on the fact that there is no on-site systems and programming activity being performed either by IS staff or by private consultants. If the original vendor who supplied the software has access to the institution's operating or program software through an offsite networking hookup offsite, more extensive review procedures must be employed. This workprogram also should not be used whenever the institution under examination provides any significant IS services to another nonaffiliated institution(s). The FFIEC IS Examination Workprogram should be used for IS examinations when more detailed examination steps are appropriate.

The community financial institution workprogram contains general instructions and a series of work steps to be performed before answering questions. There is a cross-reference table at the end of the work program that relates the location of the primary initial reference for that work steps. The reference is pointed to the appropriate section, by the chapter and page number located at the bottom center of the page.

INTRODUCTION

Technological advances in recent years have given rise to smaller yet more powerful computer systems.

Effective interaction with most systems now requires only a modicum of computer knowledge and takes place through menu programs or graphical user interfaces. Pricing for many computer systems has decreased to a point that is within the capabilities of most, if not all, financial institutions. Many small financial institutions (community bank/thrift) have taken advantage of technological advances and purchased in-house, or turnkey, computer systems.

Essentially, a turnkey system consists of a purchased software application that, when installed on appropriate hardware, typically requires only modification of parameter tables and loading of an institution's financial data before processing can begin. The parameter tables may be interest rate tables, service charge tables, interest charge methods, etc., that programs will retrieve values from to apply in various data manipulations. Generally, no additional program modification must be accomplished. Turnkey systems vary in complexity and some may require extensive data processing knowledge to operate and maintain. Progressive institutions with aggressive business plans may require several experienced data processing personnel to manage the systems as they become more complex. Ultimately, the decision to acquire a turnkey system should be made after careful analysis and evaluation of pertinent facts.

Many of the issues related to larger, more complex information systems discussed in other sections of the Information Systems Handbook are basic tenets and also apply to smaller systems. The remainder of this chapter will discuss issues germane to smaller, turnkey systems.

RATIONALE FOR ACQUISITION

Many factors may give rise to the desire to obtain a turnkey system. Generally, the need or desire to acquire a turnkey system will result from one or more of the following reasons:

- Financial institution operations and advancement into new commercial areas may be inhibited by the servicer's inability to adapt.

-
- The current servicer is not responsive to institutional request for enhancements.
 - The cost of services rendered the financial institution have become excessive.
 - The servicer may be ending services partially or completely.

In the latter case, financial institution managers may be faced with the need to acquire processing capability rapidly, especially if the servicer is curtailing operations due to financial failure.

EVALUATION OF SYSTEM REQUIREMENTS

To facilitate the evaluation and decision process, a committee consisting of users and managers should identify system requirements. It is important that an institution's end-users be involved in the process. They can provide valuable information regarding current problems and what would enhance processing. Not including them may result in their failure to provide important information and could result in resistance to change. Additionally, there must be a thorough understanding of the initial and continuing costs associated with the acquisition of an in-house system. Normally, the committee's findings are reported to the board of directors for ultimate review and acquisition approval.

FEASIBILITY STUDIES

Very few financial institutions rely on manual systems for information processing. Most either receive data processing services from a third-party provider to meet their particular needs, or they have acquired an in-house system. As previously mentioned, the decision to acquire a turnkey system should be supported by a thorough analysis and evaluation of relevant facts. This is probably the most critical step in the entire process. It is in this step that the evaluation and recommendation for system approval will be completed. Faulty analysis may result in an undesirable system that fails to meet management's expectations. The inaccurate determination of costs involved may adversely affect an institution's earnings and ultimately capital. For those reasons, among others, the cost of a thorough feasibility study will be minor in comparison to the funds spent on a system that does not fulfill expectations.

Feasibility studies are the prime method for evaluating the suitability of solutions to particular

problems. Refer to initiation of a feasibility study, management should have a clear understanding of what the current problems are and what constitutes the desired remedies. Without this information, effective solution is unlikely.

The degree to which any feasibility study needs to be conducted will depend on an institution's specific needs. The study may be completed by in-house personnel, but it is not unusual for specialized consulting firms to assist. System vendors for turnkey solutions also may provide consulting services. However, management must remember that some consultants have an interest in increasing the installed base, and may not be unbiased in the recommendation of a system.

HARDWARE AND SOFTWARE CONCERNS

Software Evaluation

System acquisition should focus on the most important part of the system – the software. Too often the emphasis is on finding a computer and the importance of the software is overlooked. Software consists of a set of instructions that can be executed by a computer. The software should be thoroughly evaluated to determine that it will meet the institution's current and future needs. Once an institution has tentatively identified a suitable software package, a good step to take would be to contact current users of the product and ascertain their satisfaction. User groups also may provide good information on the functionality of the product and responsiveness of the vendor to users' needs. Examiners should review management's software evaluation process to gain a further understanding of selected packages' suitability.

Audit Trail Considerations

Software for financial institutions should provide the capability of auditing transactions if financial information in monetary accounts will be manipulated. Clear audit trails should be produced as transactions take place. The ability to obtain reports detailing transaction activity should be part of the standard software. The reports should contain the date, time, type of transaction, terminal from which the transaction was initiated, and the identification of the person initiating the transaction. The software's intrinsic ability to produce adequate reports, or the existence of an add-on package through which suitable reports can be generated, should be evaluated by examiners. The lack of adequate report generation

capabilities will limit the value of the information system to management and should receive adverse commentary in the IS Report of Examination.

Software Costs and Use Rights

The cost of software will vary with the complexity or size of the institution. Normally, software is not purchased and the financial institution obtains no ownership rights. Rather, the software developer licenses the user and allows the user certain rights to the software. Depending on the particular software, license rights may reach multiple thousands of dollars and will be granted for a specific period of time. There may also be an annual fee associated with the software use. Periodically, new versions, or releases, to the software will be provided.

Program Modifications

Since most turnkey software packages are developed for the express purpose of installing it in multiple institutions, most vendors offer custom program changes to adapt the package to meet certain user needs. Some minor alterations may be provided at no charge, but users should expect to incur additional expense for most software changes. Periodic vendor initiated enhancement to the software should be expected. These changes may result from the institution of new laws and regulations that require them. Or, the changes may be at the request of user groups that are experiencing problems or want software enhancements. Such changes may be included without additional cost in the periodic routine software upgrades as long as they are improving the generic software package and are not particular to any single institution.

Hardware Selection

After a suitable software package has been selected, a determination on the necessary hardware can take place. This normally will not pose a significant problem from the selection standpoint. Since the software vendor will know what hardware best runs the software, some selection decisions may already be made. Many of the software vendors either sell the entire package which includes hardware, or work closely with other vendors that do. Costs and services vary and management should evaluate suppliers to obtain the most favorable terms.

Purchasing and Leasing Hardware

Hardware, like software, may be leased or purchased. The initial cost of purchased hardware may be significant and will depend on the system design. Amortization of the cost for such equipment usually should take place over a period of time not longer than seven years. A review of the actual method employed by a financial institution should take place during an examination.

Leasing takes on more favorable attributes in the opinion of some managers. The system cost can be apportioned over the lease period and remains somewhat constant. Then, at the end of the lease period, management normally has the option to continue utilizing the equipment on an extended lease, purchase the equipment at a specific value, or arrange for new equipment. Managers and examiners should thoroughly review the acquisition of equipment. This is especially necessary when the institution is upgrading hardware systems, and the old hardware will be purchased by the current or new vendor as part of the sales agreement. Such transactions have given rise to excessive costs for new equipment based on inflated purchase costs. If abuses are found, such transactions should receive unfavorable commentary in Reports of Examination. Additional guidance may be found in the FFIEC Supervision Policy 6 (SP-6), Interagency Statement on EDP Service Contracts. Although SP-6 primarily focuses on service providers, the same general problems may exist in lease agreements or repurchases of used computer equipment.

Maintenance Concerns

Computer systems are predominately electronically oriented, but many of the system components have mechanical or moving parts. This gives rise to the need for a sustained maintenance program to minimize the probability of an equipment failure. Normally, operators can perform the majority of routine maintenance on equipment such as tape drives, reader/sorter devices, and other mechanically oriented equipment, but some required maintenance is best performed by individuals that specialize in such matters. Management should be aware that a continuing commitment is made when hardware is acquired through lease or purchase. Replacement and maintenance cost considerations should be a part of

any decision to purchase or lease equipment.

Vendor Stability Evaluation

The acquisition of a turnkey computer system generally entails significant costs and requires certain levels of knowledge regarding the system. Financial institution management may place a considerable reliance on the various vendors for technical support and overall assistance. Some of the knowledge necessary to evaluate a particular vendor's stability may be gleaned from overall dealings with the vendor during the product evaluation phase of system selection. However, if reliance will be placed on the vendor for continued support, an evaluation of the vendor's ability to provide the necessary support should be made. This can best be accomplished by reviewing the financial strength of the vendor. This may be complicated by the very nature of the vendor.

If the vendor is part of a larger organization, financial statements may not segregate that particular segment of operations making the evaluation difficult. Companies that are not publicly traded may not willingly provide access to financial information. This does not imply that these companies are not strong and capable of withstanding business cycles. But, the inability of management to adequately evaluate these companies should indicate caution is necessary when determining their continued support, potential. The evaluation should not end once the acquisition has taken place. Periodic evaluation should take place for any support vendor management relies on. Appropriate documentation to substantiate the review should be maintained. Management's analysis should be reviewed during examinations.

Facilities

In addition to ensuring that appropriate equipment and software are obtained, management must be concerned with providing an adequate environment in which to process work. Depending on the nature and extent of the system chosen, alterations may entail only a slight rearrangement of work areas. If a physically larger system is acquired, the construction of a segregated area with a special environmental control system may be necessary. Some controls and features are discussed in the following paragraphs.

Equipment Floor Plans

The location and arrangement of the system should take into consideration the work patterns of people

and the flow of documents. It is not advisable to have large numbers of people consistently traversing the area where computer operations take place. Such presence provides a heightened potential for accidental damage to systems and the potential to lose information. Preferably, the computer system should be in an area that is away from the general public and access to the area restricted to only necessary personnel. Workflow, or document flow, also should be considered to enhance efficiency. Arranging the processing operation and equipment to facilitate workflow should result in a smoother and less time consumptive environment.

Noise Considerations

The physical environment may require special considerations. With the exception of any reader and sorter equipment, these smaller microcomputer based systems are not generally noisy. High speed impact printers are exceptionally noisy. If they are utilized, sound dampening covers may be necessary. As a result of the size and type of various peripheral devices in use, significant noise may be created during normal operations. Without a special facility to house the equipment, the noise may be disruptive to other workers in the area.

Environmental Controls

Small systems, some of which may be run on very powerful microcomputers, will generally only need an environment that is suitable to humans. These systems are very tolerant of a wide range of temperatures and conditions. Larger systems may require special environments where climate and humidity control are necessary. Computer systems also are capable of generating significant amounts of heat. Failure to adequately maintain suitable temperatures within the operating environment may result in system failure and loss of data.

Fire Detection/Suppression Considerations

No matter what the system size, adequate protective systems must be maintained. Fire protection systems for smaller, microcomputer based systems, may consist of hand-operated fire extinguishers. These extinguishers should not be dry chemical. The release of the contents of the extinguisher could cause more damage than the small fires they are designed to extinguish. Larger, specialized facilities most likely will require a more sophisticated system such as halon or its replacement gas, FM200. These central

suppression systems are costly to install and maintain. They may often be supplemented by hand-held extinguishers.

Library Facilities

Adequate facilities for tape and disk storage should be provided. The storage facility also should be protected by a fire protection system and have limited access. Because this area will house numerous different tapes, disks, or cartridges, each item should be clearly marked to ensure that the contents are known.

Physical security

No matter what the system size, adequate security for the facility must be in place. Fire detection systems should provide local notification and it is preferred that they also notify either a monitoring entity or fire department. Intrusion alarms should be connected to a 24 hour monitoring facility. Some smaller institutions have installed infrared sensing devices that monitor and provide alarm when temperature changes are detected. These are primarily intrusion detection devices, but because a fire would result in heat increases, the sensors will detect them also. While a fire would trigger an alarm, it would signal an intrusion alarm and a fire would most likely increase in intensity before the fire department could be notified and respond. Management should evaluate the need for protective systems. Generally, a schematic diagram of security and fire suppressions system will be available and sufficient in detail to allow an evaluation of these systems.

DATA CONVERSION

For institutions that have records on a manual system, loading information into the computer system for the first time will entail a significant amount of effort. The conversion may require and will probably be best completed by a phased conversion where specific files are computerized based on a targeted completion date. Due to the potential for significant losses during a conversion, extreme care must be taken to ensure that a thorough reconciliation of balances from manual records to computer records takes place. Where an in-house computerized system currently exists and a different system is being installed, conversion will consist of transferring data from one system to another. Most vendors will assist in the conversion and provide necessary programs to complete the conversion. As with the initial loading

from a manual system, adequate reconciliation from the old system to the new system must take place. Because of the speed at which computer to computer communications can take place, the conversion may require considerably less time to fully implement. A thorough review of the conversion should be conducted during an examination. Particular attention should be given to the reconciliation process between systems. Management should consider parallel processing, if the capability exists. This would further ensure that the new system was functioning properly before shutting down the old system.

CONTRACTING FOR SERVICES

Because of the nature of many institutions, numerous services are contracted out. Any service provided to an institution for the acquisition, installation, or conversion of information should be pursuant to a written contract. The contract should cover all pertinent points and fully set forth requirements and expectations. Specific language should be included to facilitate an evaluation of the product or service relative to the terms of the contract for acceptance purposes. (Refer to Chapter 22, IS Servicing Providers/Receivers, for additional information on contracts).

DISASTER/CONTINGENCY PLANNING

Information and Data File Backup

No matter what the size and complexity of the system, adequate backup of system information must take place. Instructions for backup operations should be present and adherence to the requirements evaluated. Written procedures should outline the various frequency for backups and specify retention period for records. All media contents should be clearly marked. Retention periods should be sufficient to ensure that no more need for the data can be anticipated before its destroyed. Management should ensure the backup media is stored in an alternate location. Under no circumstances should the repository for the backup media be the same location as the system from which it was taken. This would result in an unacceptable exposure to loss of all data and could render backup media useless.

Emergency and disaster recovery planning must be accomplished by all institutions and should consist of institution-wide recovery planning. FFIEC SP 5, "Interagency Policy on Contingency Planning For

Financial Institutions” provides general guidance to financial institution managers regarding contingency planning.

Emergency Plans

Emergency events may result in the temporary inability to utilize financial institution facilities, including the computer operations area. Example, would be a bomb threat or loss of power to the facility. Both of these events will disrupt data processing activities, but not preclude the resumption of the activities within the same facilities in a reasonable, and normally short, period of time. The disaster recovery plan would be directed toward situations in which the facilities may no longer exist or the perceived inability to utilize regular facilities for a protracted period of time exists. A major fire, earthquake, or flooding could render facilities unusable for significant periods of time. Under these conditions, management would need to re-establish operations at another location.

Emergency planning should consist of actions to be taken to prevent the loss of life, injury of personnel, prevent loss of data within the system, and when possible, conduct an orderly shutdown of the computer system. The plan should be written and all personnel should be familiar with it. There should be an annual test of the emergency plan to ensure all personnel know their responsibilities. The emergency plan may be a part of the disaster recovery plan.

Corporate Contingency Recovery Plan

The disaster recovery plan should be a financial institution-wide plan including recovery of information systems at a secondary site. The need for an elaborate plan will be dictated by the level and complexity of the information systems in use. The plan should be written and clearly state who has the authority to order the re-establishment of operations at the backup site. Since the declaration of a disaster may entail a significant fee where a structured recovery site is involved, this power should not be arbitrarily granted. Often, the plan will limit this to one person. While, in theory, this may seem suitable, criteria should be established that will let other people act. Otherwise, the implementation of plan may be delayed while attempts to contact the designated person take place.

Regular Testing Program

Familiarity with the disaster recovery plan is

essential. When an emergency takes place, resumption of operations in a familiar environment is anticipated. The move to a backup site that would be required in a disaster is a re-establishment of operations in an entirely different location. Participants in recovery operations must know exactly what part they play and what actions they must carry out. It is important that the plan’s annual testing incorporate all recovery team members to the extent possible.

Board of Director Involvement

Senior management and the board of directors should review and approve the plan. A subsequent review and approval of the plan should be conducted annually. This can be accomplished by ensuring that after the plan’s annual test any necessary updating takes place. The test results and updated contingency plan can then be submitted for approval. All reviews and approvals should be noted in the institution's official records.

Examiner Review

Examiners must thoroughly review both the plan and any tests conducted to determine if they are realistic and implementable. Failure to have an acceptable plan or conduct an annual test will normally require adverse comments in the Report of Examination.

CONTINUING ISSUES AND CONCERNS

Audit Program

The need for audit exists in any system, manual or computerized. However, special skills may be required to effectively audit computerized systems. Some institutions may lack sufficient audit expertise to conduct effective information systems audits. When such is the case, external assistance from qualified audit providers should be obtained. Most institutions will possess the capability to implement some form of an internal audit program covering information processing systems. At a minimum, institutions should have processes to verify that interest calculations remain correct after parameter changes and that access to the information system is limited to those who require computer use. Examiners should thoroughly understand the level of audit performed for the information systems in use.

Audit Software

Audit software may be included as part of the particular software system a financial institution

purchases. There also are also audit software products produced by third party vendors for many systems. Audit software provides the capability to produce reports or records that can be used to verify information within the computers databases. Additionally, there are numerous report writer and query programs that can be used to produce audit reports. The query facility within the OS400 operating system is a prime example. Most examiners are familiar with the direct verification process for deposit or loan accounts. The verification notices are one product produced by audit software. When in use, all query report formats and programs utilized for auditing purposes should be strictly controlled. Ensuring the integrity of these programs is of paramount concern.

Systems and Program Maintenance

The nature of most turnkey or small computer systems implies that there is no programming activity at the institution. This is most often the case. Some people may consider the setting of program parameters, such as interest rates, to be programming. However, unless the alterations to the system result in actual changes to the logic, or way the system manipulates data, it is not considered programming. Program maintenance in the turnkey environment normally consists of updating particular vendor programs with a disk or tape sent to the institution for installation. In some institutions, management may allow the vendor to upgrade the programs via a remote communications package. In these instances, all remote access via dial-up modem should be pre-approved by management, and the upgrade activity needs to be thoroughly documented in a log book. In any case, parameter changes and program upgrades must be controlled. Only under extraordinary circumstances should the vendor be allowed unaccompanied access to the computer system. Once a computerized system is established, any changes to the system should only take place after management's approval has been obtained. Specific procedures, preferably written, should be in place, and adhered to, for any parameter change or system upgrade. These procedures should include a post-implementation review of the parameter changes made to ensure they were correctly applied. For example: changes in the calculation of interest, terms of instruments, etc. must be proper. This review should occur no later than the day following the change and be performed by an employee with a clear understanding of what was modified and that the expected results were achieved. This form of verification also may be coordinated

with the audit department. Records of changes made should be maintained and available for examiner review.

Software Escrow Agreements

For institutions that do not purchase a source code, vendors usually have arranged for it to be held by a third party. The code would be available to the users under conditions specified in the license or escrow agreement. Examiners should be aware that when this situation exists, an audit of the software in escrow should take place annually. The audit should verify that the software held by the escrow agent is the latest version and that the source code is compilable and executable. Since vendors also offer some custom modification to the software packages, examiners should ascertain that copies of the custom code or altered programs also are safeguarded. Otherwise, the financial institution may be unable to restore the exact code to perform operations from the escrowed software.

While many vendors do not provide the source code to the institution, some vendors do place the source code on the system to facilitate corrections, enhancements, and resolution of problems. Examiners that encounter the source code on the institution's system, where programming does not take place, should determine why the code is there and how it is secured or access to it is restricted.

New Release Installation

As discussed earlier, most vendors periodically will update software to take advantage of new processes, correct deficiencies and problems, and generally improve the application's utility. Sometimes, financial institutions do not upgrade to the new version. When this condition is observed within a financial institution, examiners should determine the reason management has chosen not to install the latest version. Failure to install periodic releases may result in difficulty when the institution has to install more recent versions with required changes in regulatory or other requirements. It is possible that before installing the most recent version, that all previous releases must be installed. This can be very time consuming and a sudden, significant expense for some institutions.

Many software vendors require installation of the periodic update that is normally near the end of the calendar year. This is due to changes normally made to facilitate end-of-year processing. Often, the new

version must be installed within a specific time period. This is frequently tied to the cut-off date after which the previous version may no longer be supported.

Appropriate Report of Examination commentary should be made where the failure to upgrade to most recent versions of software is discovered.

Continuing Evaluation and Planning

Management should periodically evaluate the capabilities of the information system relative to the institution's current business plans. Capacity planning should ensure that the growth in financial information does not exceed the system's capacity to maintain the information. Some software vendors stratify their software and license it to be used in financial institutions with specific levels of assets and or accounts. It is too late to begin planning when the recommended levels are exceeded. Management would be forced to react to a potentially critical event.

Because no system is designed to be the last one, management must have a system replacement plan. All systems will have an effective usefulness, if not functionally, then economically. Management must remain vigilant to the need to upgrade or replace outmoded technology and software. Failure to remain aware and take the necessary steps could result in an insecure or less than cost effective system.

Training

As with the need to maintain software and equipment, personnel also must receive periodic training to remain effective. Many features in computer systems are underutilized or not used at all due to the lack of understanding. Even smaller systems often provide features that could provide more utility if they were better understood. Management should provide periodic systems' training and ensure whenever new equipment or software is obtained, adequate training is provided to a sufficient number of employees.

Regulatory Examinations

The installation of computerized information systems may result in the institution being subjected to regulatory examinations. During these examinations, an assessment of the audit coverage, management, systems and programming, and computer operations activities will take place. An overall rating will

normally be assigned to the Information Systems activities. These examinations usually will be conducted in accordance with the FFIEC guidelines with results reported to management at the conclusion of the examination. Examiners should communicate their findings with management during the examination process to facilitate better communication and corrective actions.

EXAMINATION PROCESS

FFIEC Community Financial Institution IS Workprogram and IS Report of Examination

The FFIEC has adopted a format for examining turnkey systems, the IS Workprogram for Community Financial Institutions. Each agency is responsible for guiding its examiners through the workprogram. All necessary areas are addressed by the workprogram, but it should be considered an evaluation tool only, not the end of the process. Negative answers on the workprogram may not indicate an undesirable condition in every institution. Compensating controls may be in place and alleviate the need for controls specified in the workprogram.

The FFIEC also has adopted a specific report format for Information System Examinations. The report has an open and confidential section. Generally, completion of the report is guided by FFIEC standard with minor deviation allowed by the various agencies.

Shared Application Software Reviews

Shared Application Software Reviews (SASRs) for the most widely used turnkey software packages are produced by FFIEC member agencies and are available for examiner use. These reviews provide a good overview of package features, and any systemic problems with the software. For areas identified as potential problems, examiners should look for compensating controls. They also may indicate problems that arise when particular hardware is used to run the package. Because the revision of most turnkey software is enhanced and known problems periodically corrected, examiners should not rely solely on problems noted in SASRs for report comments. A determination as to the existence of the problem in a specific institution must be made. Additionally, the SASRs are not, under any circumstances, to be released to the institution. They are for internal FFIEC member agency use only.

Segregation of Duties

Small financial institutions, the predominate users of turnkey systems, may lack adequate staffing to fully segregate duties and responsibilities. In such cases, additional precautions and controls should be established to ensure system integrity. These measures can consist of rotation of duties and additional audit coverage. Examiners should ensure

these measures have been established and adhered to, but remember to be reasonable when requesting additional controls. At a minimum, management should ensure that an adequate number of employees receive training on the system to minimize dependence on any one person. To facilitate communications with vendors, a primary and alternate contact should be designated to handle system problems.