

In recent years, microcomputers or personal computers (PCs), have become more prominent in the business environment. They are now being used, not only as word processors and access devices to other computers, but also as powerful stand-alone computers. As such, information processing has evolved well beyond the traditional central environment to distributed or decentralized operations. This trend has offered substantial benefits in productivity, customization, and information access. However, it also has meant that those control procedures, previously limited to the central operations, must be reapplied and extended to the end-user level.

End-user computing is the transfer of information processing capabilities from centralized data centers onto the user's desktop. End-user computing systems may range in size and computing power from lap-top notebook computers, to standalone personal computers, client-server networks, or small systems with sufficient computing power to process applications for a financial institution. Small systems entirely supported by a hardware or software vendor are referred to as turnkey systems (not to be confused with PC/LAN systems). Control considerations discussed throughout this section generally apply to all end-user computing systems.

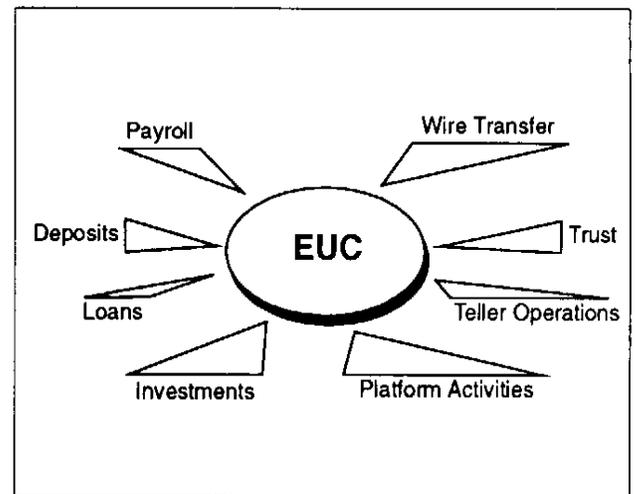
In many cases, end-user systems are linked in distributed processing networks. The ability to decentralize the data processing function is largely a result of the development of powerful microcomputers or PCs. Microcomputers are now powerful enough to process significant applications when used as stand-alone systems. These systems also can be connected to a host computer and configured to serve as data entry/display terminals. In this terminal emulation mode, information can be passed between the host and the PC with the processing occurring at either machine. Therefore, it is very important that controls over the downloading and uploading of data are in place and adequate.

Linking several microcomputers together and passing

information between them is called networking. A system configured in this manner is commonly called a local area network (LAN). When linked by a network, end-user computing offers several advantages to financial institutions, including:

- Low cost relative to other platforms.
- Efficiency through the sharing of resources.
- Ease of expansion for future growth.
- Enhanced communication capabilities.
- Portability.
- Data availability.
- Ease of use.

*Figure 16.1
End-User Computing Activities Overview*



Although end-user computing systems provide several advantages, there are increased risks to data integrity and data security. These risks include:

- Difficulty in controlling access to the system.
- Lack of sophisticated software to assure security

and data integrity.

- Insufficient capabilities to establish audit trails.
- Inadequate program testing and documentation.
- Lack of segregation of duties.
- Inadequate System Development Life Cycle (SDLC) procedures.

As the trend toward distributed processing continues, financial institutions should have proper policies, procedures, and reporting to ensure the accurate and timely processing of information. The controls in an end-user computing environment should be no different from the those implemented in a traditional mainframe information system environment. In this new environment, local management and staff should assume responsibility for the information assets of the organization. Institutions that design reporting systems to fit their specific needs also have a competitive advantage.

CONCERNS

Technology, using microcomputers as end-user computing devices, has taken data processing out of the centralized control environment and introduced computer related risks in new areas of the banks. However, the implementation of these new information delivery and processing networks has out paced the implementation of controls. Basic controls and supervision of these computer activities often have not been introduced, or expected, at the end-user level. The technological advantages, expediency, and cost benefits of end-user computing has been the primary focus. Recognition of the increased exposures and the demands for expanded information processing controls has lagged. These concerns for data protection and controlled operations within the end-user environments must be addressed to minimize risks from:

- Incorrect management decisions.
- Improper disclosure of information.
- Fraud.
- Financial loss.

- Competitive disadvantage.
- Legal or regulatory problems.

End-user computing is recognized as a productive and appropriate operational activity. However control policies for data security and computer operations, consistent with those for centralized information processing functions, need to address the additional risks represented in the end-user computing operations.

Bank management is encouraged to evaluate the associated risks with its end-user computing networks and other forms of distributed computer operations. Control practices and responsibilities to manage these activities should be incorporated into an overall corporate information security policy. Such a policy should address areas, such as:

- Management controls.
- Data security.
- Documentation.
- Data/file storage and backup.
- Systems and data integrity.
- Contingency plans.
- Audit responsibility.
- Training.

Responsibilities for the acquisition, implementation and support of such networks should be clearly established (See Chapter 25 for additional information on FFIEC SP-3: Joint Interagency Issuance on End-User Computing Risks).

STANDARDS

Acquisition Criteria

The increased use of microcomputers, end-user computing platforms and microcomputer networks in financial institutions requires management to establish appropriate standards and policies governing

the acquisition, implementation, and support of end-user computing. Management should establish acquisition standards, for both hardware and software, as uncoordinated purchases could result in excessive costs, redundancy, incompatibility with other systems, and servicing complications. End-user computing acquisition policies may include:

- Feasibility studies at the user/management level.
- Development of a centralized purchasing unit.
- Corporate wide guidelines for user departments.

Microcomputer acquisition policies should eliminate duplication of effort by user departments and save money. However, new policies should be introduced carefully to user departments. Management should avoid cumbersome or inflexible policies that may be ignored by microcomputer purchasers. A set of balanced microcomputer acquisition policies should serve the needs of both management and users (SP-3: Joint Interagency Issuance on End-User Computing Risks).

User Standards

User standards and effective employee training programs are crucial to prudent microcomputer use. Although the microcomputer may not need a specialized temperature-controlled environment, there are other security considerations. For example, the microcomputer location should discourage unauthorized access and passwords should be required to access PC standalone and shared programs.

Standards relating to the microcomputer software process can help prevent and detect errors or the fraudulent manipulation of data. Misuse and inadvertent errors can erase programs and data on microcomputers resulting in serious problems. User standards should describe the risks involved in operating microcomputers. A well informed user should understand the need for controls and recognize that microcomputers contain sensitive data.

HARDWARE AND SOFTWARE SELECTION

Software selection may limit the institution's hardware alternatives. For example, some software is

designed to operate on a specific group of computers or requires a hardware configuration that only can be supported by certain vendors. Before selecting hardware, a financial institution's management should prepare a list of requirements for comparing alternative hardware proposals.

The two most important considerations in selecting hardware are the machine's capacity and its performance capabilities. Evaluating capacity requires a review of the institution's present and future needs, including projected growth, types of automated applications, anticipated new products, and future management information requirements.

A decision also must be made whether to purchase or lease the equipment. This decision should consider the costs of each method, including the tax and earnings consequences, and the effect of technological advances on future hardware costs and performance. Although either method is acceptable, the decision to acquire a system should be made only after conducting a comprehensive review of the institution's present and future objectives within the context of its strategic plan. This should include systems compatibility and interconnectivity for future expansion purposes. In the absence of such a review, management might purchase an inefficient or inadequate computer system, which could result in a substantial loss if the equipment had to be sold or upgraded. Costs for hardware and software generally should be amortized over 4 to 7 years. Otherwise earnings may be misstated.

Software Selection

Selection of the right software for each business function is critical to overall microcomputer success. Because of the variety of software available for microcomputers, the following questions should be addressed in establishing software selection guidelines:

- What applications are to be processed?
- What is the appropriate use of licensed software?
- What access control mechanisms are included in the software?
- How should in-house developed software be controlled?

-
- How much user involvement is needed in selecting the software?

Senior institution management should be involved in establishing proper criteria for software purchases. Although microcomputer software is relatively inexpensive, it is an investment that benefits the organization. A commitment by management to establish comprehensive software selection criteria should help maximize the benefit of all software purchases.

Physical Protection

Financial institutions should protect the computer equipment. Because of their portability, microcomputers are especially at risk of being stolen or misused. The location of microcomputers and the types of applications being processed should determine the extent of physical security that is required. At a minimum, microcomputers should not be located in areas that afford easy access to customers or unauthorized employees. Whatever physical security the financial institution determines is appropriate, the effectiveness of the security measures depends on employee awareness, and management's enforcement of the controls.

Care also should be taken to shelter the equipment from environmental risks. For example, the microcomputer should not be placed under a sprinkler valve that can be triggered by a fire in another area of the building or in a flood-prone basement. Surge protection devices should be used to prevent damage due to fluctuations in power.

Every financial institution should have equipment to prevent fire damage. In a small institution, such equipment is often limited to portable fire extinguishers. The cost of a more extensive fire protection system, while desirable, may not be justified.

OPERATIONS

End-user computer operations is a microcosm of the traditional data processing center. Senior management should work with local managers to develop policies and standards for applications development, documentation, change controls, and security. Refer to the appropriate sections of this

handbook for discussions of these topics.

A key element in maintaining a properly controlled operations environment is the segregation of duties between each area. However, small institutions may find that separation of duties is not practical because there are few employees. In such circumstances, it may be possible to establish an acceptable control environment by instituting compensating measures, such as the rotation of duties.

Important controls in end-user computer systems reside in the user departments. The person in the user department who initiates transactions should not be responsible for reviewing output and balancing reports. Audit trails should be provided for all posted transactions, including file maintenance. Transaction reports should be printed and made available for review. The need for the user departments' involvement in reviewing and balancing reports cannot be overemphasized. This is one of the best control mechanisms for an end-user system.

DISASTER RECOVERY/CONTINGENCY PLANNING

As end-user computer systems increase in computing power and processing capabilities, it is important to assess the adequacy of disaster recovery and contingency plans for these systems. The need for contingency planning is related to the importance of the applications being processed. Critical data maintained on PCs must also be protected through proper back-up procedures. As financial institutions begin to process more critical applications on end-user systems, the contingency plans for these systems should become more closely aligned with those of larger systems.

Special consideration should be given to adequate back-up frequency for data files. Management often undervalues information on PCs and fails to implement proper back-up routines.

NETWORKS AND TELECOMMUNICATIONS

Financial institutions with microcomputers and other end-user computer systems rely on telecommunications to interconnect the organization's computing functions. Telecommunications allows users to communicate and share information and

resources. In decentralized processing, this type of communication is critical to assimilating information from various organizational units to use in the management decision-making process.

If the system is a LAN located within a single building, the risk from external sources, such as tapping telephone lines, is reduced. The primary concern is the adequacy of controls over the desk top functions and the type of information that can be accessed. These concerns usually can be addressed through the operating system software or by controls programmed into the applications software.

The capabilities of each end-user system and the controls present to protect the integrity of the financial data and software should be determined. Many systems will have activity logs that show user activity. If such logs are available, a knowledgeable supervisor should review them for unusual activity (See Chapter 15 for additional information on firewalls and other forms of hardware, software, and network controls).

SMALL SYSTEMS

In some financial institutions, end-user computing systems may include a large microcomputer or minicomputer with peripheral equipment that processes all applications for the institution and functions as a small data center. The hardware manufacturer or the software vendor may assume full responsibility for the system design and installation, and supply all necessary hardware, software, and documentation. This type of system is referred to as a turnkey system. Small system control considerations generally apply to all end-user computing systems.

Financial institutions with small systems may purchase or lease software packages to process such applications as demand, savings, and time deposits; loans; investments; and general ledger. In many cases, these software packages also include a central information file. Application software for turnkey systems is usually obtained from the hardware manufacturer or from an independent software vendor.

Vendor software generally consists of standardized

programs. Customized enhancements may be available for additional charges, but may not be provided in a timely manner. Most standardized software packages offer a variety of options, including various user reports, account types, and interest rate and fee options. Such options are usually table-driven, giving an institution's staff the ability to change them without requiring programming changes.

When a financial institution acquires application software from a vendor, both parties will usually sign a software maintenance (including purchase or lease agreements) agreement. Under the agreement, the financial institution usually will be entitled to receive all new software releases, with installation and operation assistance provided by the vendor for a set fee. New releases may contain requested changes from users, modifications to comply with changing legal and regulatory requirements, or corrections to previous versions. Some software applications also may require annual maintenance updates. Releases may be provided according to a set schedule or issued only as needed. Some vendors will not provide programming support, unless the user has installed all of the previous releases. Therefore, a financial institution should remain current with software releases to ensure vendor programming support and compatibility with other users.

In financial institutions with little or no programming capabilities, emphasis in the selection process should be placed on the careful analysis of all available software packages that could include a cost/benefit feasibility study. Some key questions to consider include:

- Does the software meet the present and future needs of the institution?
- What reports and records does the institution need?
- Does the system include audit reports?
- Does it have a system log or an on-line log?
- Are there adequate program controls for data integrity?
- Does the software contain access control features such as password protection of various applications?

-
- How are the passwords generated, and can limitations be placed on their length and composition?
 - Can the systems be configured to force periodic password changes?
 - Are passwords stored in encrypted form?
 - Is the software installed in other financial institutions?
 - If it is, visits to other institutions with a similar operation may be beneficial in evaluating the system.
 - If it is not, it may be more difficult to determine whether the software will meet the institution's needs, and backup arrangements may be more difficult. In such circumstances, extra care is required to ensure that the new software performs as expected before the conversion process is completed.
 - What is the cost of the software?
 - Is there an additional cost for executing the software at multiple workstations?
 - Does the software vendor supply programming support?
 - If yes, at what cost?
 - If no, how will program problems be corrected?
 - Is the vendor readily available to support the software?
 - Does the vendor have the financial capacity to provide long-term support?
 - Is the software documented?
 - Does the financial institution receive or have the right to obtain source programs and program documentation?
 - Does the institution have the right to modify the software?
 - If so, how does this affect the future warranty and vendor support?

- If not, how does this affect plans for future operations?
- Do contracts for buying or using the software protect the rights of both parties?
- Is the software compatible with other computers?
- May it be used to service other institutions?
- Is the software easy to use?
- Are the operating and user guides adequate and are they written in clear, easy-to-understand language?
- Is adequate employee training provided?

Often, user groups are formed to address issues concerning a particular software package. Where possible, institutions should strongly consider joining such groups.

Program (System) Change Control

Many vendors request dial-up access to provide on-line programming support. While this method may assure that modifications are made in a timely and efficient manner, the financial institution is subject to the risk that the person who requests access over the telephone is not a bona fide vendor employee. In order to control this risk, a financial institution should implement a procedure, such as calling the vendor back at a predetermined number, to verify that the caller is an authorized vendor employee.

Any changes to application software by anyone other than the vendor may void warranties. As a general rule, in-house modifications should be made only at the direction of the vendor. If the modifications are vital to the institution and the vendor is unwilling or unable to make them within a reasonable time, senior management should be made aware of the problem and the potential ramifications of not making the modifications.

Third-party Escrow Agreements

Over the past few years, the software market has become extremely competitive, and many software vendors are concerned about the confidentiality of their programs. In order to retain more control over their products, some vendors prefer to give only

object programs (machine language programs) and user guides to their customers. Another method of maintaining confidentiality which allows the financial institution access to the documentation, is to establish a third-party escrow agreement. Under this arrangement, an escrow agent retains a copy of the source programs and supporting documentation in safekeeping with instructions to deliver the materials to users in the event the vendor is unwilling or financially unable to support the software.

Provisions that are usually incorporated into an escrow agreement include:

- A definition of acceptable software maintenance.
- Conditions that must be present before the customer can obtain the source programs and documentation.
- The media in which the source programs will be released; e.g., magnetic tape, disk, or hard copy.
- Arrangements for auditing the escrow arrangement.
- An assurance, which includes a provision for periodic testing, that the most current versions of the source programs and documentation will be held by the escrow agent.

At a minimum, the software documentation held by the escrow agent should include system flowcharts or a system narrative, program source listings, program narratives, file and record layouts, descriptions of individual fields within the records, and calculation routines. Portions of this documentation may be included with the user guides that are provided to the financial institution. These guides also should cover transaction codes and descriptions of input forms and output reports.

Without the source code and the program documentation, program changes are virtually impossible. As long as the financial institution can be assured of access to both, a separate contract programmer may be employed to meet any crises arising from the vendor's failure to provide programming support. Having this recourse substantially reduces the potential risk to the financial institution.

Third-party Programming

The option of hiring a third-party programmer to develop unique software or modify existing software to meet the financial institution's needs is not common, because of the proliferation of existing software packages. Although this option is a viable alternative, serious problems can occur when:

- There is a misunderstanding of the requirements between the programmer and the financial institution.
- There is complete reliance on a single individual for programming support.

An experienced programmer, given enough time and money, can create reliable software packages. However, for a financial institution to control the development process properly, it should determine whether the programmer is qualified to perform the work; establish limits on the amount of money it is willing to spend; make periodic payments only as the work is completed; and establish realistic time frames for completing the work. These conditions should be incorporated into a contract that details the responsibilities of each party. When the programming is completed, it should be thoroughly tested under all conceivable conditions to ensure that output is reliable and that each program performs as anticipated. In addition, the financial institution should ensure that program documentation, user guides, and source programs are properly developed and readily available. The institution should ensure that their fidelity bond coverage also extends to contract programmers.

System Software

Each computer system has a collection of programs and procedures known as system software. The system software includes the operating system, system utilities, and compilers or interpreters. The basic purpose of each component is described as follows:

- Operating system – Master program that controls operation of the computer system. It supervises the execution of programs, allocates storage, and handles input and output devices. Some examples are OS/400, Unix, MS/DOS, OS/2, and Pathworks.

- System utilities – Programs that perform repetitive functions, such as creating, deleting or altering files, and copying files for backup.
- Compilers – Programs that translate source programs that are written in high-level languages, such as COBOL, to object programs that the computer can then execute.
- Interpreters – Programs that function similarly to compilers and are used for translating low-level languages into machine language. Unlike compilers, this process must be done each time a program is executed.

Periodically, updates to the software are released and installed by the financial institution. The financial institution may be supplied with numerous manuals describing the system and its capabilities, but it may need to know little about the system software other than control options for password protection, security codes, access control features, and activity logs. Options available in the system should be properly documented, along with management's decisions about the use of such options.

Appropriate controls should be established for source code, compilers, and data-altering utilities. One obvious way to prevent tampering is to remove compilers and data-altering utilities from the system, but this option is not always possible. Certain systems use these utilities during normal production runs. Other systems do not use compilers, but require that the source code be kept on the system and translated into object code each time a program is executed. Controlling risk in these systems may prove especially difficult. In such cases, an activity log should be automatically generated by the system. The logs should record the execution of application programs, system utilities, compilers, user activity, and should provide the nature of the activity, the date, the time, and where the activity was initiated. The activity log should be generated frequently and reviewed routinely by a supervisor or auditor, who has a complete understanding of the information presented in the log. Unauthorized use of data-altering utilities should be investigated immediately.

Even if a compiler or the source code is not on the system, some vendors provide these items upon request. If a financial institution has these items in its

possession, they should be placed under appropriate dual access controls. When these programs are needed, their use should be monitored and documented.

RISK AND CONTROL CONSIDERATIONS

See Chapter 25 for additional information on FFIEC SP-2 and its Appendix: Uniform Interagency Rating System for Data Processing Operations.

SECURITY

Risks

- Software may not be available to provide adequate security for client/server environments.
- Adequate physical security for critical hardware components may be lacking due to the distributed nature of the environment and the slow development of security conscious cultures in the client/server arena.
- Inadvertent or intentional unauthorized end user access to software and data presents greater risk of loss in client/server environments due to a potential dependence on the end user to implement some system functions.

Controls

- Adequate steps should be taken to prevent unauthorized access, use of, or changes to, systems or data.
- Procedures should be implemented to ensure the privacy and confidentiality of information.
- Management must review security reports.

COMPUTER OPERATIONS

Risks

- Disaster recovery and business continuation plans may be incomplete or outdated due to more frequent changes to hardware and software resources.
- Exposure to system failures may be increased due to easier software virus infiltration in a distributed environment.

- Incomplete hardware and software inventories could result in additional exposures in the form of unidentified network operations and/or the lack of adequate insurance coverage.
- Management information systems that rely on client/server systems could become incomplete or inadequate due to the lack of adequate operational controls.

Controls

- Procedures should be adequate to ensure the timely, accurate, and complete processing of information.
- Management should ensure that critical systems and operations are recoverable in the event of a disruption in service.

IMPLEMENTATION AND MAINTENANCE

Risks

- Internal control considerations could be neglected due to the shortened time frames commonly found in the development of client/server systems.
- System failures resulting in weaknesses not identified in pre-implementation testing are more likely to occur than in mainframe environments.
- There are increased risks from unauthorized modification of application programs due to the distributed location of the client and its applications.
- Application development costs may consistently be underestimated if a system development life cycle methodology is not used.
- Failure to re-engineer the work flow in the design phase of the application may limit management's ability to optimize the benefits from this technology.

Controls

- Appropriate procedures, including a system development life cycle methodology, should be included in new and existing client/server systems.

- Audit should have involvement in the SDLC process.

SYSTEM SOFTWARE

Risks

- In this heterogenous environment (i.e., consisting of multiple platforms), there is an increased vulnerability to incompatibilities in installed software versions. Thus modifications may cause inconsistent operating results.

Controls

- Management should ensure that systems are properly tested and approved and that modifications are properly implemented.
- Management should determine that adequate version control procedures are properly implemented.

DATABASE MANAGEMENT SOFTWARE

Risks

- Database integrity may be corrupted by deficiencies in the quality of the implementation and the administration of database management systems.
- Lack of database integrity is of greater concern due to concurrent updates of distributed databases which may not have properly established locking capabilities.
- Unauthorized access to the data could occur as a result of inadequate database administration or improper data ownership.

Controls

- Management should implement controls to ensure the integrity and confidentiality of transactions.
- Management should ensure that systems are properly tested and approved and that modifications are properly implemented.
- Management should determine that adequate version control procedures are properly implemented.

-
- Management should determine that the database management system has adequate recovery capabilities.

MIDDLEWARE

Risks

- System integrity may be adversely effected because of multiple operating environments attempting to interact concurrently.
- Lack of proper software change procedures across multiple platforms could result in a loss of system integrity.

Controls

- Management should implement controls to ensure the integrity of the client/server networks.
- Management should ensure that systems are properly tested and approved and that modifications are properly implemented.
- Management should determine that adequate version control procedures are properly implemented.

CONCLUSIONS

This section reviewed many of the controls that

should be evaluated in financial institutions with end-user computers. In evaluating these systems, auditors and examiners should assess whether the institution's established standards, policies, and procedures are adequate to control the inherent risks that are present in end-user computing environments. In addition, auditors and examiners should determine the degree to which the users adhere to those standards, policies, and procedures.

Acquiring an end-user computer system requires careful planning and the active involvement of senior management. Professional organizations in both data processing and the financial community offer training that provides a nontechnical approach to understanding computers. With this background, senior management can better guide the acquisition and implementation of end-user systems. The failure to understand the capabilities and limitations of automated data processing systems has produced costly and unsatisfactory results for some institutions.

End-user computer systems will continue to proliferate as a relatively low-cost option for meeting the data processing needs of financial institutions. These systems are already valuable tools to support managerial objectives in many financial institutions. The value of these tools is increased by an effective system of controls that ensures the data integrity and security of information processed on these systems.