Handbook: EDP Examination Handbook   **Section:** Administrative
Subject: End-User Computing   **TB 29**

July 10, 1989

End-User Computing

RESCINDED

> *Summary:* This Bulletin supersedes R67-1 which is hereby rescinded. The contents have not changed. This Bulletin is meant to provide guidance to management for evaluating potential risks, and for implementing adequate control practices and responsibilities in end-user computing environments. It is expected that management in each FSLIC-insured institution utilizing end-user computer systems will implement controls consistent with guidelines offered in this Bulletin.

For Further Information Contact:
The FHLBank District in which you are located or the Compliance Programs Division of the Office of Regulatory Activities, Washington, DC.

Supplementary Information:
The following Bulletin is an Interagency Policy Statement issued by the Federal Financial Institutions Examination Council (FFIEC) and adopted by the Federal Home Loan Bank System.

Thrift Bulletin 29

Purpose

The purpose of this issuance is to alert management of each financial institution of the risks associated with end-user computing operations and to encourage the implementation of sound control policies over such activities.

Background

In recent years, microcomputers, or "personal computers," 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.

Concerns

Technology, using microcomputers as end-user computing devices, has taken data processing out of the centralized control environment and introduced the computer related risks in new areas of the institutions. However, the implementation of these new information delivery and processing networks has outpaced 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, and
- 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.

Institution 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 back-up,
- systems and data integrity,
- contingency plans,
- audit responsibility, and
- training.

Responsibilities for the acquisition, implementation, and support of such networks should be clearly established.

The appendix to this issuance provides more detail regarding the risks and suggested controls for end-user computing and other computer related activities. Additional control recommendations can be referenced in the FFIEC EDP Examination Handbook.

TB 29

Policy

It is the responsibility of the board of directors to ensure that appropriate corporate policies, which identify management responsibility and control practices for *all* areas of information processing activities, has been established. The existence of such a "corporate information security policy," the adequacy of its standards, and the management supervision of such activities will be evaluated by the examiners during the regular supervisory reviews of the institution.

Attachment

— *Darrel W. Dochow, Executive Director*

RESCINDED

Risks and Controls in End-User Computing

Microcomputers, in the end-user computing operations, are being used basically for three purposes:

1) as word processors,

2) as communications terminals with other computers (to transmit or receive information in their databases), and

3) as stand-alone computer processors.

These three functions require different control objectives, based on the risks associated with the activity. Each function requires certain operational type controls such as physical security, logical security, and file back-up. However, the more pronounced risks involve those operations using microcomputers as stand-alone processors.

While word processing and terminal communications also require strong controls, programming support for the operating software and applications systems generally remain centralized or is a vendor responsibility. In end-user computing, the user is often engaged in program development, in addition to information processing. This may involve the creation of programmed software from an original design or building customized routines from specialized vendor software. Regardless, the control techniques for the programming, its testing and its documentation are necessary to ensure the integrity of the software and the production of accurate data.

In addition to the programming activity, the end-user environment supports computer processing, which may be totally separate from centralized controls. Information may be downloaded from the main databases and reprocessed by the end-user. Data may also be originated for processing in this structure.

Regardless of the source, the resulting information is relied upon by management for decisions impacting corporate strategies and customer relationships. The integrity of the data becomes no less important than had the data been produced through more sophisticated computer processes. Likewise, the need for control at the micro level remains equally important.

Impacts

The failure to properly implement a uniform set of controls on the end-users of microcomputers, consistent with those controls required in a mainframe data center, can create two broad categories of risks:

1) the corruption or loss of data and/or program software, and

2) impediments to the efficient operation and management of the institution.

The quality of data is paramount to the successful management of any institution. Should the data, or the systems which produce that data, be corrupted, whether intentionally or unintentionally, financial loss is highly probable. Data corruption could result from three basic causes: error, fraud, or system malfunction.

In addition to accuracy, management requires the timely availability of data. Inefficiencies, caused by poor operational controls, can further impede the production of information and result in financial loss. Regardless of the source, poor quality information and operations can adversely impact the institution in a number of ways:

- Management Error - Inaccurate or incomplete data can adversely influence institution management decisions. Delays in information availability can also adversely impact corporate strategies.

- Inadvertent Disclosure - Human error, fraud, or system malfunction may result in proprietary institution data, customer data, or program software being disclosed to unauthorized persons.

- Competitive Disadvantage - Problems in the production of accurate and timely information can place the institution at a competitive disadvantage. Delivery of services, customer confidence, and management decisions could be impaired.

- Legal Problems - Errors in the production of data or wrongful disclosure of data may result in legal actions against the institution by its customers, consumer groups, competitors, and regulators.

- Regulatory Problems - Failure to produce timely and accurate data can cause the institution to be in violation of regulatory requirements, subjecting the institution to regulatory penalties.

- Monetary losses to the institution can arise from deliberate manipulation of the data (fraud), missing or erroneous data (leading to costly incorrect decisions), or various inefficiencies in the operation of the system.

Controls

There are basic controls which should be present in any level of computer operations. These controls should already be present at the centralized data center. The evolution of microcomputer based systems has not eliminated the need for these basic controls, but has shifted the focus of control to the end-user level.

Some of these basic control standards that need to be implemented in microcomputer-based systems are:

Appendix to TB 29

Policies and Procedures

Control requirements for microcomputer use need to be addressed by management in its internal policies and procedures. Policies and procedures should be in writing and should define what steps are to be taken to protect the institution's microcomputer systems. Management should also designate responsibility within the institution to monitor microcomputer system acquisition and use. The purpose of this function should be to help prevent redundant uses of microcomputer systems and to ensure that there is the required degree of compatibility among hardware and software systems in use throughout the institution.

Program Development and Testing

Before a new system is developed or purchased, the user should have a clear understanding of the specific needs being addressed by the proposed new system. Alternatives should be reviewed by the user and analyst to ensure that the best solution is selected. Development should be done with the aim of producing a system that is easily modified and maintained by someone other than the original developer. Finally, the completed system should be subject to rigorous testing to provide assurance that the results produced are valid and reliable.

Program Changes

Just as with larger systems, microcomputer systems must be adapted to meet changing requirements and circumstances. Modified programs should be subject to many of the same controls as newly-developed systems. Most important among these is the requirement that there be thorough testing of the modified system. In addition, accurate records should be maintained describing the change, the reasons for the change, and the person responsible for making the change.

Documentation

Documentation is a potential problem in microcomputer-based systems. There is a tendency for these systems to be highly personalized, with one person fully responsible for the development, testing, implementation, and operation of a set of programs. The successful use of a microcomputer-based system and the production of specialized data may depend on the continued presence of this one person. An adequate level of documentation helps to prevent an over reliance on the knowledge of this one person. This is particularly needed should revisions to programs be required. Documentation standards should define acceptable levels of program, operating, and user documentation. In addition, there should be an enforcement mechanism to guarantee compliance with standards.

Data Editing

The development or purchase of microcomputer systems should be done with adequate attention given to the need for data editing routines. These routines are important to help ensure that data entering the system is error-free and not likely to result in erroneous output. This control is important whether the data is being manually entered into the microcomputer or electronically transferred or "downloaded" from another system. In the case of data being "uploaded" to a mainframe, additional controls may be required at that level to guarantee the integrity of the data being transferred.

Input/Output Controls

Microcomputer systems that are used for the processing of information with a direct monetary impact on the institution or its customers may require that additional data controls be established. At a minimum, these controls may include the requirement that there be a segregation of duties between the input of information and the review of that information in processed form. This control may be extended to require that a formal reconcilement be done by the reviewer of the processed information. In more sensitive situations with a significant dollar impact, there may be a requirement that certain functions be performed under dual control. The need for these types of input and output controls should be established during the early stages of program development. These special requirements need to be described in detail in the program documentation package.

Physical Access Restrictions

The location of microcomputer systems outside of a physically-secure data center can permit unauthorized access to programs and data files used on these systems. The use of physical access restrictions complements the logical access restrictions discussed below. Basic steps would include the secure storage of diskettes or other magnetic media containing the programs and data for a particular system. In addition, since documentation on what a system does and how it is being used can provide important information that can be used to compromise system security, this information should also be secured. Finally, there should be adequate restrictions over physical access to the hardware itself, so that it is protected from unauthorized use, vandalism, and theft.

Logical Access Restrictions

Just as in larger application systems, the need exists to identify those individuals who will be permitted

access to the microcomputer system's capabilities. In addition, there may be the need to differentiate between functions allowed for certain individuals, ranging from an inquiry capability for many persons to an override and correction capability for a few supervisory personnel. Normally, these restrictions will be in the form of password controls. Standard password related control procedures, such as frequent changes and reporting of exception conditions need to be established to provide for effective access restrictions.

Backup and Contingency Planning

For each operational system, adequate plans should be made and precautions taken to ensure that users can adequately recover from damage to the hardware, software, and data. For some systems, an ina-bility to process during recovery may mean that work can be held for later processing. For other systems, a manual backup may be appropriate. For some time-critical, highly automated systems, arrangements may have to be made for data reconstruction or for processing on other hardware. At a minimum for all systems, there should be secure and remote backup storage of data files and programs. Beyond this, the backup and contingency requirements for individual systems may differ and need to be addressed separately.

Audit

The audit area should serve as an independent control reviewing microcomputer use throughout the institution. Audit involvement in microcomputer systems may begin at a general level with a review for compliance with the internal policies and procedures discussed above and may extend to detailed testing in particular areas such as the use of logical access controls. Audit procedures and workprograms should be expanded to provide for adequate coverage of microcomputer systems. Responsibility for microcomputer auditing should be clearly assigned and plans for microcomputer audits should be built into the audit schedule.

It should be recognized that this list of controls is not all inclusive of methods to manage risk. Each computer operation, whether centralized or end-user, possesses different characteristics and possibly some specialized risks. Control practices must be sufficient to minimize such risks. These recommended control features are considered *fundamental* to sound information processing.