NATIONAL CREDIT UNION ADMINISTRATION
WASHINGTON, D.C. 20456
LETTER TO CREDIT UNIONS

NCUA LETTER NO. 109 DATE: September 1,1989

TO THE BOARD OF DIRECTORS OF THE FEDERALLY INSURED CREDIT UNION ADDRESSED:

INFORMATION PROCESSING ISSUES

For your reference I am enclosing papers from the Federal Financial Institutions Examination Council (FFIEC) which outline issues and risks associated with certain computer operations.

Credit unions will continue to benefit from "distributed" processing systems if proper controls are set up, as suggested in one of the papers. Likewise, large-scale integrated systems (LSIS) are becoming more common and also require proper controls, as indicated in another paper.

Guidelines for contingency planning are also included here. Each board of directors should ensure that a comprehensive contingency plan is put in place and tested regularly. Because such planning has become crucial to credit union operations, contingency plans and test results will be reviewed and evaluated during future supervisory examinations.

For the National Credit Union
Administration Board,

ROGER W. JEPSEN
Chairman

SN: ltm
Enclosures

Federal Financial Institutions Examination Council
Washington D.C. 20006

Joint Interagency Issuance on
End-User Computing Risks

TO: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

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,
- 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.

POLICY:

It is the responsibility of the board of directors to ensure that appropriate corporate policies, which identify management responsibilities 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.

APPENDIX

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 processed 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:

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 inability 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.

Federal Financial Institutions Examination Council
Washington D.C. 20456

Supervisory Policy on Large-Scale Integrated Financial Software Systems (LSIS)

TO:

Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

Financial institutions have experienced significant problems in attempts to introduce LSIS systems.

- After 2 1/2 years in development, one financial institution abandoned $20 Million large scale integrated system!

- After 5 years in development, a major software vendor abandoned $100 million integrated system - once described as the perfect software system for regional banks!

PURPOSE:

Financial institution executives and directors should be aware of and concerned about the potential problems with LSIS. The purpose of this paper is to alert financial institutions to the risks associated with these systems and to identify management's responsibilities when entering into an LSIS project.

BACKGROUND:

An integrated software system is one in which programs for different applications--loans, deposits, retail, and wholesale--that normally are designed and operated as stand-alone programs are built from the start as related parts of a whole. They share a common language, operating system, and other technical details so that they can be made to 'talk' to each other with relative ease. More importantly, they function as one unit so that the sum of the parts is greater than the whole." 1/

Christopher K. Heaney, "Who are these guys anyway?" ABA Banking Journal, May 1986, pp. 84-85

Financial institutions are adopting LSIS in order to meet competitive pressures, increase timeliness of information, foster operational efficiency, and ease introduction of new products. A commitment to LSIS sets the course of an institution's technology, management information system, and delivery systems for several years. Successful implementation of-LSIS requires careful planning by both senior management and the board of directors.

Ineffective planning caused several financial institutions and software companies to spend millions of dollars and years of conversion and implementation time on LSIS, only to implement a portion of the system or in some cases abandon the project altogether. In many instances, the software vendors depended upon substantial ongoing investment by the financial institutions to fund the vendor's research and development process. When these projects experienced lengthy delays, the financial institutions not only suffered large monetary losses but also delays in product development and a loss in their competitive positions.

CONCERNS:

- Financial institutions have underestimated the cost, time and personnel resources required for the successful installation of LSIS. Therefore, time and cost targets should be established at the beginning of the project and closely reviewed by senior management on an ongoing basis.

- In certain cases LSIS projects were abandoned because of the financial instability of software vendors. To prevent these situations from recurring, the financial condition and viability of each prospective vendor must be considered when evaluating systems.

- Data backup and recovery measures for integrated systems are often more costly than those required for single application systems. In certain situation, the data base may require simultaneous backup. The additional costs for backup and recovery must be evaluated when determining the feasibility of LSIS.

- If the system provides for instantaneous update of information--in other words, the user has direct access to the data--existing security systems may not be adequate. Thus, data security features must be evaluated to ensure that sufficient controls exist for LSIS.

- Seemingly simple program changes can have unpredictable results in a mixed-application system. Thus, system development life cycle methodologies, which identify the sequence of activities required in the systems development process and throughout the useful life of the software, may need to be modified.

- There is an increased possibility of unwarranted data manipulation and at the same time, there is less of an audit trail in an LSIS environment. Therefore, EDP audit coverage should be reviewed at the onset to determine whether specialized audit techniques are needed.

Board of Directors and Senior Management Responsibilities

The decision to acquire or develop in-house large-scale integrated software should be preceded by a strong and independent management planning process. This should include a thorough examination of existing software performance. Also, a detailed analysis of the system's capability to meet the institution's strategic business plans is essential.

The complexity of the software and its impact on the entire organization require a commitment from top management for the project to be successful. Responsibility for the conversion should be clearly identified and established at the senior management level.

Senior management should regularly review the project's status. This improves control over the complex process of implementation and ensures completion within established time and cost targets. It is particularly important that the board continue its oversight responsibilities after implementation.

The attached pages discuss the impact and responsibilities associated with large-scale integrated systems.

APPENDIX

LARGE - SCALE INTEGRATED FINANCIAL SOFTWARE SYSTEMS

Definition and Scope

Large-Scale Integrated Systems (LSIS) are sophisticated software products which provide interconnections and facilitate the exchange of information between applications and functions. The integration architecture may be horizontal, tying together applications, such as deposits, loans, and general ledger. Alternatively, the architecture may be vertical, tying together functions, as in teller transactions being linked immediately to all operating departments. These systems are designed so that each application no longer exists individually but operates as part of a unified system. They often employ data base management technology, which increases the complexity of the system. LSIS processing may employ combinations of batch, on-line, or memo-posting methods. A variety of LSIS are being marketed and others are in various stages of development.

Small-to-medium size financial software systems whose applications simply interfaced through a Central or Customer Information File (CIF) have been operating for many years. Many of these systems have been successfully installed and have operated properly for a considerable period. These systems are not included in the scope of this issue paper, although they are sometimes described as “integrated systems.”

Advantages of Large-Scale Integrated Systems

- provide tools to increase product line and customer relationships, ultimately increasing fee income on deposit and loan services

- enable financial institutions to meet competition generated from forces outside the banking industry

- lower the unit processing costs through standardization of operating techniques

- eliminate redundancy in data files

- provide information at more points throughout the institution, enabling faster and more accurate management decisions.

Disadvantages of LSIS

- The complexity and size of large-scale integrated systems can lead to underestimation of the time and resources needed for successful installation of these systems.

- The magnitude of the installation effort requires more comprehensive management techniques and project control.

- The financial instability of the software vendor may require the institution to furnish unplanned additional financial support to maintain contemplated service levels.

- The failure to properly install the software can lead to significant losses to the institution, in terms of time and resources expended, and a decline in competitive position.

Internal Control Related Concerns

- Data Security: Data security should be addressed prior to the installation of such a system. Existing data security systems may not be adequate for a complex integrated system, particularly one using on-line real-time processing. Each individual function should be controlled, e.g. access controls, file maintenance, inquiry, and new accounts.

- EDP Auditing: A greater chance of unwarranted data manipulation and a diminished audit trail exists. Therefore, institutions should recognize the need for expanded ED; audits of this technology, especially in an on-line real-time environment.

    Absence of Acceptable Audit Trails - When a system allows the automatic generation of a transaction prompted by a prior transaction, controls must be designed within the system to ensure satisfactory audit trails. This is especially critical considering that a single transaction may generate several other transactions.

    Accountability for all transactions must be maintained through audit trails. Otherwise, system integrity deficiencies will jeopardize the software system's ability to provide a consistent product, as well as compromise internal controls.

    Absence of Comprehensive Audit Software - Existing generalized audit software may not be readily adaptable for use with large-scale integrated systems, and may not be sufficiently sophisticated to follow an audit trail of all

transactions generated by the system. Provision for audit software should be made at the time of system acquisition.

- Disaster Recovery Planning: Integrated systems have unique features which will require a thorough consideration of contingency requirements in the initial feasibility study. The complexity of the integration, horizontally, vertically, or both, may determine that current industry standards for the backup of Hardware, software, data and communications are no longer applicable. A determination should be made how the institution, as a whole, will recover and how recovery will be addressed along functional lines. Subsequently, required testing may pose cost, logistical or other problems which will have to be resolved to ensure a viable disaster recovery plan.

- Changes in System Development Life Cycle ("SDLC") Methodology: There are several significant control issues regarding the use of traditional SDLC methods with large-scale integrated systems. Current system development techniques may not permit the timely develop, and implementation of a complex system. SDLC techniques may need to be revamped to provide for increased flexibility. However, control and management methods may vary according to the complexity of the system under development.

Minimum SDLC standards should ensure that project development is sufficiently controlled to provide for the integrity of the system. Testing of various stages within large-scale integrated systems may require innovative techniques.

Management should carefully consider the cost of the extensive user involvement in the system development stage. User involvement is necessary to ensure the successful implementation of a large-scale integrated system.

Management must provide more comprehensive employee training since the adoption of a LSIS will affect all departments.

SDLC standards need to be flexible, while still providing for the maintenance of system integrity during development to ensure that a system of internal control is maintained.

Federal Financial Institutions Examination Council
Washington, DC 20006

Interagency Policy on Contingency Planning for Financial Institutions

TO: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

PURPOSE:

The purpose of this policy statement is to alert the Board of Directors and management of each financial institution to the need for contingency planning for their institution. This includes both institutions that provide their own information processing and those that receive processing from service bureaus. The policy statement also addresses issues that should be considered when developing a viable contingency plan.

BACKGROUND:

Contingency planning is a process of establishing strategies to:

- minimize disruptions of service to the institution and its customers,
- minimize financial loss, and
- ensure a timely resumption of operations in the event of a disaster.

These strategies are the same for institutions with in-house data centers and those using service bureaus.

In recent years information technology has expanded rapidly throughout the corporate structure of financial institutions. It includes operations such as central computer processing, distributed processing, end user computing, local area networking, and nationwide telecommunications. These operations often represent critical services to institutions and their customers. The loss or extended disruption of these business operations poses substantial risk of financial loss and could lead to the failure of an institution. As a result, contingency planning now requires an institution-wide emphasis, as opposed to focusing on centralized computer operations.

Additionally, there are many service bureaus that provide information processing services to multiple financial institutions. The disruption of the processing capabilities of one of these service bureaus could impact a considerable number of institutions. Accordingly, contingency planning by financial institution servicers is equally important.

CONCERNS:

Many financial institutions and servicer bureaus have not sufficiently addressed the risks associated with the loss or extended disruption of business operations. More specifically:

- Many contingency plans do not address all of the critical functions throughout the institution.
- Many serviced institutions have not established or coordinated contingency planning efforts with their service bureaus.
- Many service bureaus have not established contingency plans.
- Many contingency plans have not been adequately tested.

POLICY:

The board of directors and senior management of financial institutions are responsible for:

- Establishing policies, procedures and responsibilities for comprehensive contingency planning.
- Reviewing and approving the institution's contingency plans annually, documenting such reviews in board minutes.

If the institution receives information processing from a service bureau, management also must:

- Evaluate the adequacy of contingency plans for its service bureau.
- Ensure that the institution's contingency plan is compatible with its service bureau's plan.

The appendix to this policy provides an example of a process that management may consider in developing contingency plans. It is an outline and is not all encompassing. Each financial institution needs to assess its own risks and develop strategies accordingly. This planning process needs to address each critical system and operation, whether performed on site, at a user location, or by a service bureau.

APPENDIX

Contingency Planning Process

I. Obtain commitment from senior management to develop the plan.

II. Establish a management group to oversee development and implementation of the plan.

III. Perform a risk assessment.

Consider Possible threats such as:

- natural - fires, flood, earthquakes, . . .
- technical - hardware/software failure, power disruption, communications interference, . . .
- human - riots, strikes, disgruntled employee . . . .

Assess impacts from loss of information and services.

- financial condition
- competitive position
- customer confidence
- legal / regulatory requirements

Analyze costs to minimize exposures.

IV. Evaluate critical needs.

- functional operations
- key personnel
- information
- processing systems
- documentation
- vital records
- policies/procedures

V. Establish Priorities for recovery based on critical needs.

VI. Determine strategies to recover.

- facilities
- hardware
- software
- communications
- data files
- customer services
- user operations

- MIS
- end-user systems
- other processing operations

VII. Obtain written backup agreements / contracts.

- facilities
- hardware
- software
- vendors
- suppliers
- disaster recovery services
- reciprocal agreements

VIII. Organize and document a written plan.

Assign responsibilities.

- management
- personnel
- teams
- vendors

Document strategies and procedures to recover.

- procedures to execute the plan
- priorities for critical vs. non-critical functions
- site relocation (short-term)
- site restoration (long-term)
- required resources
  - human
  - financial
  - technical (hardware/software)
  - data
  - facilities
  - administrative
  - vendor support

IX. Establish criteria for testing and maintenance of plans.

Determine conditions and frequency for testing.

- batch systems
- on-line systems
- communications networks

- user operations
- end-user systems

Evaluate results of tests.

Establish procedures to revise and maintain the plan.

Provide training for personnel involved in the plan's execution.

X. Present the contingency plan to senior management and the Board for review and approval.

Additional guidelines are available in the section 7 of the FFIEC EDP Examination Handbook. Also, many materials on contingency/disaster recovery planning have been published by trade associations, accounting firms, And the disaster recovery industry. These can be valuable guides. to comprehensive contingency planning.