Office of Regulatory Activities

TB 11-1 rescinded 5/27/04 with the issuance of the FFIEC IT Examination Handbook's "Development and Acquisition Booklet"

Handbook: EDP Examination Handbook
Subjects: Large-Scale Integrated Financial Software System Contol Guidelines

Section: Administration
TB 11

December 9, 1988

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

Summary: The purpose of this policy statement is to alert financial institutions to the risks associated with these sophisticated software systems and to identify the responsibilities of management when acquiring, developing, and using such systems. Management in each FSLIC insured institution utilizing Large Scale Integrated Financial Software Systems should implement controls consistent with guidelines 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 11

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]

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 situations, 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

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

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 Managment 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.

Attachment

RESCINDED

Darrel W. Dochow

— *Darrel W. Dochow, Executive Director*

Appendix to Thrift Bulletin 11

Large-Scale Integrated Financial Software Sysems

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 interface 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 EDP 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 development 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.