

## Appendix F, Section 4

### Transactional System: Analysis Stage of Development

**Agency:**

Minnesota Housing Finance Agency (MHFA)

**TIS Evaluation Meeting Date:**

2 November 1998

**State Archives Staff:**

Mary Klauda, Shawn Rounds

**MHFA Staff:**

Karmel Kluender, Dave Ruch, Renata Anderson

**Agency Function:**

To provide affordable housing to low and moderate income Minnesotans through a number of resources. The agency has 160 employees and operates programs that provide financing for a variety of housing needs from multi-family housing complexes to home ownership and home improvement loans.

**System Name:**

ALPHA (existing mainframe system) and the new information system in development, based on the CORE project. The CORE project identified the process by which major business functions within MHFA need to be tracked through an enterprise-wide system. The project was called CORE because it addressed the core, or heart, of the business processes used within MHFA for meeting its mission and goals.

**System Function:**

The new system, based on CORE, will be an enterprise-wide information system encompassing all aspects of the agency's business as it builds programs, raises capital for and markets them, processes requests for funding (loan applications), disburses program funds, and finalizes all of the legal program documentation. The current ALPHA system does not encompass the entire enterprise. The programs that currently are the mainstay of single family loan activities (home ownership and home improvement) are processed on this system. Many other single family and multifamily programs and their associated business processes are tracked in a variety of desktop software packages or manually in some cases. The information gathered from the efforts in the CORE project will be used to determine the best approach to decide whether to purchase or build an enterprise-wide information system.

**System Development Phase:**

Analysis; conceptual data model and process model.

### **Background:**

The MHFA agreed to evaluate the Trustworthy Information Systems (TIS) criteria in November 1998. It was an opportune time for the State Archives (SA) since it was soon after the criteria had been developed. The SA needed an initial test case to determine how an agency might use and implement the criteria before promoting the idea as a project to the Information Policy Council (IPC). The evaluation with MHFA essentially tested the TIS criteria as a proof of concept; it validated the criteria set and gave the SA additional credibility to pursue the TIS project with the IPC. MHFA and the SA were logical partners for two reasons: 1) The two agencies had been working together since April 1998 to develop electronic records management and archival procedures, and 2) The MHFA had a new information system, based on the CORE project, in the early stages of development.

### **Evaluation Session:**

The session with MHFA was informally facilitated and recorded. At the time, the SA had yet to develop a methodology for carrying out the evaluation sessions. Since the analysis phase of system development had just been completed for the CORE project, comments regarding the criteria were based on both current/ALPHA system design and procedures and a future vision of how a new system should be designed, implemented, and supported. It also was an ideal time to begin examining system trustworthiness. The meeting lasted two hours.

### **General Reactions to TIS Criteria:**

MHFA staff found the TIS criteria useful. They appreciated having the full range of information system considerations in one document, even though many of the criteria did not apply to their agency and systems at this point. Staff had considered many of the criteria during the system analysis, but never had a structured way to document how some elements would be carried out and who would be responsible for providing and maintaining the documentation. The criteria could provide that structure.

Some of the criteria addressed issues that had not been considered fully during analysis, but ones that may become important in the future, an example being the many system security and documentation implications for handling transactions over the Internet. This will be an issue in the near future. Another benefit to the approach was documenting, in a structured way, the reasons for implementing/not implementing particular criteria considerations. For example, information systems staff had an informal understanding regarding retention of system documentation, but it was not covered in the agency's records retention schedules. MHFA staff intend to examine the criteria again as the system is developed further.

Assessing risk was the most relevant factor in determining which criteria were the most important to consider. For each of the criteria, risks of not meeting the criteria were weighed against implementation. The agency's activities are primarily financial in nature and they are audited routinely, hence financial transaction applications receive the most scrutiny and pose the highest risk. For MHFA system applications dealing with money, it was important to avoid the risk of assigning system security responsibilities to staff with an interest in the transaction or record content. Therefore, the system, as it is developed, will include procedures and personnel access

restrictions so that only limited staff with an interest in the record content will be responsible for administering system security, quality controls, audits, and integrity tests.

Information systems staff felt strongly that the criteria were important, but that the decision on whether to implement had to be based on policy and business rules that required agency management consideration and input. They stressed the need to educate system users and management on the ramifications of information technology and its application as it pertains to policy issues. For example, the agency needs to address whether the electronic record of a transaction is the official record and, if so, when it becomes reliable. Agency management and users, not the information systems staff, need to answer these questions.

### **System Documentation:**

MHFA system documentation includes data on hardware and software, its procurement, installation, modifications, and maintenance, and data on its communications networks. Further documentation considerations need to be addressed if and when client interactions take place over the Internet. Documentation does not take into account whether state- or agency-approved hardware or software is installed. As remote access and telecommuting become more common, it will be virtually impossible to monitor this.

System documentation, specifications, program manuals, and user guides are not formally scheduled in the agency's records retention schedules. There is an understanding that this documentation should be in their schedules, but it currently is not. The information systems staff have an informal retention understanding that documentation should be retained until the system is no longer used and that the system data be retained or destroyed in accordance with established records schedules, if they exist.

### **System Documentation—Policies and Procedures:**

Policy and procedure documentation includes programming conventions and procedures. Development and testing activities are recorded. Procedures for entering and accessing data; data modification, duplication, deletion; indexing techniques; and outputs are all addressed in a user manual that is external to the operating system. The identification of an official record and when it becomes reliable is something that is not within the purview of information systems staff; this needs to be addressed by users and the MHFA administration, but it currently is not.

System procedures include record formats and codes, and there are routine system back-ups. Backups are labeled and stored in a secure, off-line, off-site location, and subjected to periodic integrity testing. System staff do quality assurance and control checks and performance and reliability testing of hardware and software. They do not consult with the manufacturer. Systems do not include periodic testing of identification devices. They have addressed migration of records to new systems and media in the analysis phase. Migration issues will be considered again as CORE is developed further. Migration of records should be addressed in records retention schedules.

The agency has standard training for users and staff with access to system hardware, software, and system data.

### **System Security—User Authorization:**

The agency allows users one password with multiple sign-ons for the various systems and platforms. Individual user passwords are the same for all systems. They found that if there are too many identifiers, users tend to forget passwords or keep them someplace that is not secure (for example, a Post-It note on a computer). They would like to go to a single identifier, and, ideally, a single sign-on for all hardware and software applications.

The agency has no password dictionary, however, it does have a list of key system identifiers and passwords. They are not associated with a single person. The list includes the level of access for system users, who are allowed access to the system only at the level necessary to perform their job duties. Expiration dates for passwords are established within the system; password re-use is not allowed.

Permissions to create, modify, update, and delete records, and permissions to alter disposition codes are controlled by the applications. The agency controls user access to applications, so in effect, permission control is achieved. Access to private keys for digital signatures is not an issue at this time, but it may be at some point if mortgage applications are taken online.

### **System Security—Access and Security:**

Identification and access procedures are established and documented. User authorization forms are required before system access is granted. There is paperwork to back-up user identifiers. There is no system in place to log and track users and their online actions, nor does the system supply users with the Tennessee Warning when collecting confidential data. The Data Practices Act applies to only a few of their clients. Staff were not sure whether the Tennessee Warning was supplied in their manual paper-based system.

There are insecurity-detection mechanisms in place, as well as audit and security alerts. Security procedures and rules are reviewed on a routine basis to ensure currency. Measures are in place to guard the system's physical security. Security administration staff undergo training to ensure full understanding of the security system's operations.

The agency does not control and monitor access to system documentation. This was a level of security that MHFA staff felt they could forgo because it is costly and burdensome, and they can live with the limited risk involved.

There are additional security measures in place in cases of remote access to the system. However, as more business is done over the Internet, more security is needed in this area.

### **Audit Trails:**

The agency tracks transaction information with regard to money, and there is the ability to reconstruct audit trails from log journals. The logs are kept only for a limited period of time, and they are not maintained independently from the operating system. The logs serve as a disaster recovery mechanism rather than as an audit trail. Staff view maintaining an audit trail, particularly

one that is independent from the operating system, as a very high-cost proposition. They understand its importance, but cannot justify the costs for the limited risk situations.

### **Disaster Recovery:**

There is a disaster recovery plan in place that includes hardware, software, and database procedures, but it is not comprehensive. There are procedures in place in case of loss of automation capabilities.

### **Records—Non-System Records:**

Some MHFA data comes from a federal database at the Department of Housing and Urban Development, and the system verifies the identity of the sender and the source system. System software automatically verifies the integrity of the source and is able to detect errors in transmission and informational content.

Arrival time of data from non-system sources is considered to be the same as the creation time. There is no mechanism in place to detect changes from the time a record was created in the source system to the time that it arrives at MHFA. Staff considered this too cumbersome to administer and not cost-effective.

There is no virus detection for non-system data. However, a virus may be the cause for wrong, missing, and invalid formats, and the system detects these anomalies and will not accept the data.

### **Records—Transactional Data:**

For MHFA's purposes, record content is important, record format and structure are not. The criteria and related considerations suggested imaging to them, which MHFA will not be undertaking.

The agency felt that all of the associated metadata prescribed for each record was worth considering, to some extent. For example, for each record, the date and time of receipt are considered the date and time of creation; these are not separate pieces of metadata. MHFA does not keep metadata on record format. The location of the records is essentially indexing metadata that indicates on which drive the record is stored. Metadata for the protection method exists, depending on the degree to which security is an issue for a particular record. MHFA staff will be considering how to determine indication of the authoritative version of a record and who has the authoritative version of the record.

The agency has had difficulty with assigning unique identifiers to each record. Though it has tried to enforce this, different and multiple identifiers get assigned by program staff for various reasons.