

## **Appendix F, Section 5**

### **Transactional System: Transition to a Different Platform**

**Agency:**

City of Minneapolis

**TIS Evaluation Meetings:**

February through May 1999

**State Archives Staff:**

Mary Klauda, Shawn Rounds

**Minneapolis Staff:**

Sandra Allshouse, Caroline Bachun, Marsha Haagenson, Shirley Janssen, Merry Keefe, Mary Pedersen, Myron Rademacher, Carol Rogers, Bert Sletten, Craig Steiner, Linda Webster

**System Name:**

Human Resource Information System (HRIS) based upon PeopleSoft software

**System Development Phase:**

Analysis

**Summary of TIS Evaluation Work:**

The State Archives (SA) began collaborating with city of Minneapolis staff in February 1999 on the “authentication” (i.e., establishing the trustworthiness) of a new Human Resource Information System (HRIS) under development at that time. The HRIS Authentication Team included the HRIS administrator, the city clerk, the city records manager, a records management consultant, an assistant city attorney, and department representatives from Human Resources, Benefits, Payroll, Inspections, and Information Technology.

As a first work item, the group formalized a project rationale and developed initial team objectives (appended to this report). Several driving issues were identified, including the problem of duplicate records, difficulties in identifying the Office of Record and official records, lack of paper documentation of certain transactions, and questions as to the trustworthiness and acceptance of HRIS electronic records. Team objectives fell into two main areas: establishment of the trustworthiness of the HRIS with respect to team-determined levels of risk, and the development of a model for future authentication projects, including mechanisms for oversight, approval, and continued audits. Meeting these objectives, the group anticipated, would not only help to ensure the integrity of the city’s electronic records, but would also begin paving the way for the acceptance of the city’s electronic records in legal and audit situations. Furthermore, establishing a framework for future authentication projects and then following through with consistent application would have the broad effect of boosting user confidence in the city’s computer systems.

The team asked for assistance in applying the criteria for trustworthy information systems developed by the SA. To this end, SA staff members attended several team meetings, leading members through the criteria on an item-by-item basis, and asking whether each was relevant, already in place, or planned for future inclusion. Responses were recorded in chart form and shared with group members to elicit feedback and facilitate the HRIS development and authentication process.

During the early team meetings, the issue of whether and how risk should be included in the process was discussed. All members agreed that it was important to consider the potential exposure that the city could face if a computer system and the records it produces are considered untrustworthy. The group created and analyzed several risk models prior to selecting one for use.

The initial risk model proposed utilized a high-level decision-assessment process to determine the level of effort required to authenticate a system. The first step of the decision process questions whether the system is unique. If the system is unique, it receives the strictest examination. If the system is not unique and not used by others as trustworthy, it receives slightly less rigorous scrutiny. If it is not unique and is used by others as trustworthy, then it undergoes the least examination. The team created a preliminary model of the decision process to test the validity of the approach. Although they ultimately abandoned this model because non-uniqueness and usage are not true indicators of trustworthiness, the team acknowledged the usefulness of the exercise for raising important issues.

After review and discussion, the team decided to adopt a more complex and detailed approach to risk during the examination process. Tools were created to identify, document, and track decisions. The team began by altering the SA chart, first moving the broad considerations into a second, separate table. Then, the format of the main table was altered. Whereas the form was originally keyed to the criteria set, the team re-numbered the items so that each could be referred to by a unique identifier. Criteria deemed not applicable to the HRIS were removed and those remaining were grouped into the following categories: Documentation, Security, Audits and Audit Trails, Disaster Recovery Planning, Record Content and Metadata, and Records Management and Data Practices.

Columns were added for "Risk" and "Responsibility." "Risk" was sub-divided into "Category" and "Level," while "Responsibility" was broken down by "Human Resources," "Benefits," "Payroll," "Information Technology," and "Records Management." The risk categories were: Health and Safety (associated with physical injury or property damage); Security/Sensitivity of Data (associated with exposure of private or confidential information); Legal Liability and Regulatory (associated with increase and loss of legal cases and violations of laws and/or regulations); Fiduciary Responsibility (associated with failing to meet responsibilities and obligations to employees, residents, and taxpayers); Financial (associated with direct and indirect financial loss).

The team undertook a two-pronged approach to risk assessment. First, members determined for what areas the system would be the system of record. In consultation with staff from the city's

Risk Management Unit, they then began identifying system-associated risks, liabilities, and special concerns with the understanding that unacceptably high levels of risk would demand further examination of the corresponding parts of the system. Next, team members looked at each of the criteria, assigned it a general risk area, and examined it with respect to the likelihood of the risk occurring given the present system controls. Criteria were assigned a “Low” categorization if it is unlikely that the risk would happen, “Medium” if the risk could conceivably occur in some circumstances, and “High” if the risk might occur.

Continuing the assessment process, for each criterion the group determined which functional area(s) was responsible for gathering and/or maintaining the necessary supporting documentation and providing a written summary to the team. Team members from each responsible area were then asked, for each applicable criterion, to describe how the criterion was already being met or to indicate how it would be within a given time-frame. A “Status” column was added to the criteria table to track progress over the period from June to September.

A sub-group was formed to evaluate the sufficiency of the responses and documentation provided by each functional area. After determining that it lacked the expertise to make such judgements, the sub-group created a self-warranty procedure to document compliance. It was decided that, in the future, team members representing the functional areas of the system will be asked for their signatures acknowledging that they agree to meet the SA trustworthy information system criteria, and that they have created, or are maintaining, the proposed level of documentation with respect to foreseen risks. The signed self-warranty forms will also be sent to the department heads responsible for the HRIS system. The HRIS team felt that this two-level sign-off appropriately puts the burden of determining sufficiency of documentation on the departments involved rather than on the group. The team hopes to develop a more formal review process for future projects.

As of October 1999, the HRIS project was still underway, with work being done on the final report, general records retention schedules, procedures manuals, etc. The team identified records (selected for low risk level) within the Payroll, Benefits, and Human Resources departments that they would like to eliminate in paper form. The city attorney will be requested to issue a written opinion that the electronic form of the records are adequate. Future issues for the group include digital signature technology and the use of signatures (e.g., determination of when they are actually necessary). As well, the examination process highlighted the need to develop procedures to validate the correctness of the information being entered into the system.

The HRIS team was generally pleased with the criteria, the process they developed, and the application of risk when evaluating systems, although the group felt that prior to applying the SA examination process to other systems, it would need to streamline the risk analysis process. After final review, they hope to implement the system examination process city-wide by making it a requirement at the earliest system development phase when Requests for Proposals are sent out to vendors.

## **HRIS Project Rationale**

The rationale for addressing the authentication of the HRIS system is primarily based on issues identified in work products created during the development of the HR portion of the City General Records Retention Schedule and the HR File Conversion Project. The issues raised during these projects are typical of issues that exist in other computer and record systems in the city. The issues identified in the HR projects include:

1. The same records are maintained in multiple locations (Service File, Central HR File, Department Personnel Files, Supervisory Files, and HRIS system records—PeopleSoft).
2. The Office of Record or Official Record could not be identified.
3. Approximately 30% or more of the records in the personnel file are input documents to the HRIS system.
4. Some departments are adding records directly to the system without creating or maintaining a paper record of the transaction.
5. An effective plan for the retention and filing of HR records could not be designed without addressing whether the HRIS records could be designated as the official record for some or most transactions (thereby eliminating the need to maintain multiple copies of paper input documents).
6. Procedures did not exist to determine whether the HRIS system was a “trustworthy system.” That being the case, records produced by the system could not be deemed reliable/trustworthy for legal/evidentiary and audit purposes.

## **Initial Team Objectives**

1. Authenticate the HRIS system and the processes /procedures used to create records to ensure reliability, trustworthiness, and acceptance of electronic records in lieu of paper. Minnesota Historical Society—Trustworthy Systems: “With electronic records, the focus should be on the system; as the information itself does not exist independently of the system, the reliability of the information will be a function of the reliability of the system. From either a legal or operational perspective, the determination of the trustworthiness of the data or electronic records will necessarily focus on the trustworthiness of the hardware, software, and procedures that produce and make them legible.”
2. Document rationale/justification and selection of criteria that will be used for HRIS system authentication.
3. Identify and document definitions relating to the acceptance or meeting of criteria. Typical terms to be defined might include:
  - a. what is reasonable or practical acceptance
  - b. what is low risk versus high risk, etc.
  - c. additional terms to be added as identified
4. Identify and document specific legal/regulatory requirements or rules that may impact the designation of the official record.
5. Review and document the system, processes, and procedures used to create and maintain records (including procedures used to create, edit, and protect the records against alteration or corruption, data practices, etc.).

6. Develop and document a framework or model that can be used for future authentication efforts for other city computer systems. The framework will include procedures that can be used to create and maintain systems that will produce records that will meet reasonable legal/evidentiary and audit standards.
7. Develop and document a framework to direct authentication oversight and approval, including the continued audit of systems that have been previously authenticated.

An anticipated outcome of the HRIS Authentication Project will be to clearly identify the official records of HRIS, the form of the record, and where the records should be maintained. The authentication of city computer systems (in general) will increase the confidence levels of users of city computer systems, help to ensure the integrity of city electronic records, and provide documentation and guidance regarding the acceptance of electronic records in lieu of paper records for legal proceedings and audit.