

Appendix F, Section 1

Data Warehouse: Operational

Agency:

Minnesota Department of Finance

TIS Evaluation Meeting Date:

25 March 1999

State Archives staff:

Shawn Rounds, Mary Klauda

Department of Finance staff:

Ellen Schwandt, Darryl Folkens

Agency Function:

To improve the performance of state government in the area of statewide financial planning and financial resource management. Goals of the department include ensuring the integrity of the state's financial resources, providing governmental financial management leadership, accurately presenting the state's financial condition, facilitating informed decision making, and improving the accountability and the prudent use of state resources. The department offers services in business administration, information management, and analytical services.

System Name:

Information Access Data Warehouse

System Function:

The Finance Department's Information Access Data Warehouse holds general ledger, accounting, and procurement data and payroll/personnel data from state agency source systems. The warehouse converts and stores, in a common storage format, selected data that is extracted from the state's payroll/personnel system (SEMA4) and the state's general ledger, accounting, and procurement system (MAPS). At the time of the evaluation, the warehouse logged 750 users each month, drawn from virtually all state agencies. It is a critical business system for many state agency decision makers. Information about the Information Access Data Warehouse is available on the Finance Department's web site: <http://www.finance.state.mn.us/index.html>

System Development Phase:

In operation since 1 July 1995. Planned move from SQL Server to Oracle; target date was 16 August 1999.

Background:

The Finance Department's Information Access (IA) Department is responsible for the warehouse system as a whole; there is joint responsibility for applications with the Department of Employee Relations and the Department of Administration. System trustworthiness had been considered, to some extent, in June 1998 when the Office of the Legislative Auditor conducted a data integrity review of the warehouse. The auditors concluded that the Finance Department had controls in place to ensure the integrity of data in the warehouse and controls to protect warehouse data from unauthorized changes.

The warehouse is a repository of data extracted from the source systems, so many of the laws and regulations (e.g., data practices act, records statutes) applying to data in the source may apply to data in the warehouse.

There are legal and preservation issues that need to be addressed as the warehouse evolves. Data access issues frequently are not well thought-out in the source systems and the problems are inherited and exacerbated in the data warehouse. Even as source system agencies address their own legal issues for information systems, there is an entirely new set of issues as data from source system agencies is joined in the warehouse. There are inconsistencies between what data is retained or purged from the source systems and the source system data in the warehouse. Warehouse records retention schedules must coordinate somehow with those pertaining to the source systems. IA staff are looking at ways to develop and implement a records disposition plan.

Since the warehouse acts in a repository capacity, it does not serve as the official place of record for any of the information from the source systems. The source systems hold the official records.

System Documentation:

The IA Department has documentation in place on the procurement, installation, maintenance, and support of system's hardware, software, and communications networks. Interconnected systems are documented; some documentation on interconnected systems may not be explicit since the system is relatively small. There are some mainframe connection security issues, and the warehouse is undergoing a security review to determine system vulnerability and ways to prevent access to the system at various points.

System Documentation—Policy and Procedures:

IA staff document programming conventions and procedures, development and testing procedures, and applications and procedures for data entry and access, data modification, data duplication, data deletion, and indexing techniques.

There is documentation on warehouse system record formats and codes. There is limited documentation on source system record formats and codes. IA staff rely on the source systems to provide users with information on what codes appear in the tables.

IA staff routinely back-up the system; backups, stored off-site and off-line, are subject to periodic integrity testing. They also routinely perform quality assurance and control checks on data. For

example, there are checks to ensure that data cannot be loaded more than once. New software is installed in a test mode, with nothing being put online without first going through a test environment. There are measures in place to ensure that identification devices are functioning properly and that staff with access to the warehouse system have had security checks. The warehouse has its own computer room and its locks are changed frequently. IA staff perform quality assurance and control checks of storage medium. Eventually, the system will register when hard drives and tapes fail, triggering an automatic notification.

There is documentation on plans to migrate data to new systems, but it does not include procedures for all aspects of the migration. IA will be moving warehouse data from SQL Server to Oracle in the near future. Issues remain about which data to archive. IA staff realize the importance of retaining all parts of the data sets, but they have yet to resolve how this will happen.

System Security—User Authorization:

There are documented user identification and access procedures in place. All users are authenticated before gaining access to the system, and users are assigned a unique identifier and password. Access scripts with embedded passwords are allowed for accessing source systems' batch work. There are standard password rules for minimum password length and expiration dates. There is no limit to the number of log-on attempts per session. Since access to warehouse data is read-only, there is limited risk involved. The Finance Department has staff who respond to security incidents.

System Security—System Access:

Users and IA staff are granted warehouse access only to the level necessary to perform job duties. There is a limited number of authorized staff who can create, modify, and delete records and alter their disposition codes. Users have read-only access. Only database administrators are able to modify record identifiers. The system tracks current authorized users in a database and user lists are reviewed regularly to adjust for changes in user authorization status. There is an on-going process to review staff positions for necessary security levels. The warehouse staff is small and responsibilities are fragmented among many personnel. Position responsibilities will change as the warehouse grows. Generally, staff duties and access restrictions are arranged so that no one with an interest in record content is administering system security, quality controls, audits, and integrity testing. No individual is able to compromise single-handedly warehouse security and operations.

System Security—Internal:

For internal system security, access to system disks and to the server is controlled and monitored, although access to printers is not. Because users have read-only access, there is no concern about control over the user environment. All data from source systems is treated as secure data while it is being archived, purged, or moved from system to system. Once data is loaded into the warehouse, it is subject to system security. There are procedures in place for sanitization and secure disposal of hardware, software, and storage media when no longer needed. Security procedures are reviewed on a regular basis as necessary. Measures are in place to safeguard the system's physical security. IA staff felt that internal security issues such as facility structure and heating are very important, and that they were not examined thoroughly at the beginning of

system development. They are now rectifying physical structural problems that may have been avoided.

System Security—External:

System users currently access the warehouse with full password rights. IA staff are considering moving the warehouse to a web-based user environment. When that happens, it will be very important to do a risk assessment to look at all of the security implications. There is virus detection in place on desktop computers for external system data; it is not known whether that is the case with the servers.

Audit Trails:

IA staff can run trace files and do high-level usage reporting. For instance, they can determine how many people have accessed the warehouse and for what types of reports. Oracle tools may allow closer examination of usage in the future. IA staff operate under the assumption that the users are the owners of the data in the warehouse. Their interest in having audit trails is for performance and information management purposes only, not as a true auditing tool.

Disaster Recovery:

The warehouse has a database recovery function that is reviewed and tested periodically. There is no plan in place for the entire operating system. Although staff know they can recover from a disaster event, and have done so in the past, there is a need for a more complete and formal plan. IA staff still need to identify hardware, connections, and off-site hardware platforms. There is an opportunity to implement a comprehensive disaster plan when they move to Oracle.

Data Warehouse—Specific Considerations:

IA staff document procedures and gather metadata as data is extracted from the source systems and as data is cleansed and transformed for the warehouse. There is minimal data cleansing that occurs and cleansing and transforming procedures are described. In preparing for the move from SQL to Oracle, more issues on documenting and describing data transformation have come to light. Users can view all metadata and documentation including table and view definitions, element definitions, table information, indexes and elements, join keys, dictionaries, sample metadata reports, and source system information. The metadata is readable by anyone, but can be manipulated only by IA staff.