PERFORMANCE AUDIT

OF

TECHNOLOGY SERVICES AND THE AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF EDUCATION

May 2001

31-594-00

EXECUTIVE DIGEST

TECHNOLOGY SERVICES AND THE AUTOMATED INFORMATION SYSTEMS

INTRODUCTION

This report, issued in May 2001, contains the results of our performance audit* of Technology Services and the Automated Information Systems, Department of Education.

AUDIT PURPOSE

This performance audit was conducted as part of the constitutional responsibility of the Office of the Auditor General. Performance audits are conducted on a priority basis related to the potential for improving effectiveness* and efficiency*.

BACKGROUND

Technology Services (formerly known as Data, Research, and Technology Services), headed by the chief information officer, provides data processing services to the Department. The mission* of Technology Services is to provide leadership and technology services that continually improve the quality, accessibility, and use of electronic information to meet the needs of government agencies, schools, and the Michigan education community. Some of the primary responsibilities of Technology Services include providing local area network* (LAN) and technical services, ensuring that all applications run smoothly in the client-server* and data warehouse environment, coordinating training and technical support for the Department's users,

* *See glossary at end of report for definition.*

and developing and maintaining the Department's Internet and intranet web pages.

During our audit period, the Department moved its automated systems off the mainframe computer and onto its LAN as client-server systems. The Grant Accounting System, Federal Letter of Credit System, J20 System for Food and Nutrition Programs (J20 System), and State Aid Management System (SAMS) are examples of systems that were moved to the LAN.

Executive Order 2000-9 established the Center for Educational Performance and Information as a temporary agency. Among its other responsibilities, this agency will be responsible for establishing a single repository of educational data that will replace the Education Data Network* and the K-12 Database*.

For fiscal year 1999-2000, Technology Services had appropriations of approximately $6.4 million and was authorized 37.2 full-time equated positions.

AUDIT OBJECTIVES, CONCLUSIONS, AND NOTEWORTHY ACCOMPLISHMENTS

Audit Objective: To assess the effectiveness of the Department's general controls over the management, development, and security of its automated information systems.

Conclusion: The Department's general controls over the management, development, and security of its automated information systems were limited in their

* *See glossary at end of report for definition.*

effectiveness and should be improved. Our assessment disclosed two material conditions*:

- The Department had not established a comprehensive information systems security program (Finding 1).

  The Department agreed with the corresponding recommendation and informed us that many improvements to security have already been implemented and further improvements will be made.

- The Department had not established effective program change controls (Finding 8).

  The Department agreed with the corresponding recommendation and informed us that it is in the process of establishing effective program change controls.

In addition, we identified reportable conditions* related to the effectiveness of information technology, technology services organization and staffing, LAN access controls, physical security controls, standardization and documentation of network configuration, system development methodology and system documentation, LAN backup and recovery controls, and business resumption plan (Findings 2 through 7, 9, and 10).

Audit Objective: To assess the effectiveness of the Department's internal control* over its automated information systems.

Conclusion: The Department's internal control over its automated information systems was generally

* *See glossary at end of report for definition.*

effective. We determined that data was accurately processed by the automated information systems and that, in general, payments were properly calculated and paid to the recipients. However, we identified reportable conditions regarding system access controls, SAMS processing controls, completeness and accuracy of processing, and audit trails (Findings 11 through 14).

Noteworthy Accomplishments: We conducted a survey of a sample of school districts to obtain their opinions about the Grant Accounting System, J20 System, and SAMS. The survey disclosed that the school districts were generally satisfied with the systems. The survey also disclosed that the school districts were very satisfied with the timeliness with which payments were received.

AUDIT SCOPE AND METHODOLOGY

Our audit scope was to examine the information processing and other records of the Department of Education's automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Our methodology included examination of the Department's information processing and other records for the period October 1, 1998 through September 30, 2000. Our methodology also included developing a preliminary risk assessment of Technology Services and the automated information systems. We used this assessment to determine which systems to audit and the extent of our detailed analysis and testing. We reviewed internal control over the Grant Accounting System, Federal Letter of Credit System, J20 System, and SAMS pertaining to (a) general controls, which included management and organization controls, system development and documentation controls,

program change controls, and LAN controls, and (b) application controls, which included data input, data processing, and data output controls.

AGENCY RESPONSES AND PRIOR AUDIT FOLLOW-UP

Our audit report contains 14 findings and 15 corresponding recommendations. The agency preliminary response indicates that the Department agreed with all of the recommendations.

The Department complied with 2 of the 10 prior audit recommendations included within the scope of our current audit. We repeated 2 prior audit recommendations in this report (Findings 1 and 10) and 6 were rewritten for inclusion in this report.

This page left intentionally blank.

May 24, 2001

Mr. Arthur E. Ellis, Chairperson
State Board of Education
Hannah Building
Lansing, Michigan

Dear Mr. Ellis:

This is our report on the performance audit of Technology Services and the Automated Information Systems, Department of Education.

This report contains our executive digest; description of agency; audit objectives, scope, and methodology and agency responses and prior audit follow-up; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Complied Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This page left intentionally blank.

TABLE OF CONTENTS

TECHNOLOGY SERVICES AND THE AUTOMATED INFORMATION SYSTEMS DEPARTMENT OF EDUCATION

INTRODUCTION

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agency

Technology Services

Technology Services (formerly known as Data, Research, and Technology Services), headed by the chief information officer (CIO), provides data processing services to the Department of Education. The mission of Technology Services is to provide leadership and technology services that continually improve the quality, accessibility, and use of electronic information to meet the needs of government agencies, schools, and the Michigan education community. Some of the primary responsibilities of Technology Services include providing local area network (LAN) and technical services, ensuring that all applications run smoothly in the client-server and data warehouse environment, coordinating training and technical support for the Department's users, and developing and maintaining the Department's Internet and intranet web pages.

The Department has experienced significant turnover in the CIO position. Since fiscal year 1996-97, the Department has had five different CIOs and, at one point, went 18 months without a CIO. During our audit period, the Department moved its automated systems off the mainframe computer and onto its LAN as client-server systems. The Grant Accounting System, Federal Letter of Credit System, J20 System for Food and Nutrition Programs (J20 System), and State Aid Management System (SAMS) are examples of systems that were moved to the LAN.

For fiscal year 1999-2000, Technology Services had appropriations of approximately $6.4 million and was authorized 37.2 full-time equated positions.

Automated Information Systems

During our audit period, the Department operated the following systems, among others, on its LAN:

a. Grant Accounting System

   The Grant Accounting System is an automated payment system used by the Office of Financial Management and Administrative Services to administer over 16 federal grant programs that provide financial assistance to the State's school districts. The system also provides for monitoring of grant allocations, approvals, and payments. School districts input expenditures and payment requests through the Michigan

Education Information System* (MEIS). The current Grant Accounting System was implemented in October 1999 on the Department's LAN. The system previously resided on a mainframe computer. In fiscal year 1998-99, the Grant Accounting System processed approximately $800 million in payments.

b. Federal Letter of Credit System

The Federal Letter of Credit System, developed in 1997, is an automated system that helps the Department's Office of Financial Management and Administrative Services determine current federal cash draw needs in compliance with the federal Cash Management Improvement Act. It also allows for consistent reporting of federal grant activity. The system incorporates data obtained from the State's Management Information Database* (MIDB) and the Department's historical letter of credit grant data to determine cash draw needs. It distributes the federal revenue into the State's accounting system (the Michigan Administrative Information Network* [MAIN]) and creates the schedule of expenditures of federal awards. In fiscal year 1998-99, the Federal Letter of Credit System drew approximately $800 million to be distributed to subrecipients.

c. J20 System

The J20 System is an automated payment system used by the Office of School Support Services to calculate meal reimbursements to public and nonpublic schools and residential child care facilities that are enrolled in the National School Lunch Program, School Breakfast and Snack Programs, and Special Milk Program. The J20 System also calculates meal reimbursements to nonresidential child care centers and family or group day care homes that are enrolled in the Child and Adult Food Care Program. Data is input by the school districts through MEIS. In 1998, the Department began the development of a new LAN-based system to replace the existing mainframe system. During our audit, the processing of applications continued to be done on the mainframe computer, although the processing of claim payments had been moved to the new LAN system. In fiscal year 1998-99, the system processed approximately $212 million in payments.

d. SAMS

The State School Aid Act (Sections 388.1601 - 388.1772 of the *Michigan Compiled Laws*) provides for aid to support the public schools and intermediate school

* *See glossary at end of report for definition.*

districts in the State. SAMS is an automated payment system used by the Office of State Aid and School Financial Services to calculate State school aid payments for distribution to the State's school districts. Funds are allocated to each school district based on statutory formulas. The payments include a foundation allowance* for each membership reported by school districts and also funding for categorical programs*. School districts input membership data through the Education Data Network. In fiscal year 1998-99, SAMS processed approximately $10 billion in payments. SAMS was converted from a mainframe system to a LAN-based system in 1992 and was rewritten in 1998 to a Windows-based system.

Executive Order 2000-9 established the Center for Educational Performance and Information as a temporary agency. Among its other responsibilities, this agency will be responsible for establishing a single repository of educational data that will replace the Education Data Network and the K-12 Database.

* *See glossary at end of report for definition.*

Audit Objectives

Our performance audit of Technology Services and the Automated Information Systems, Department of Education, had the following objectives:

1. To assess the effectiveness of the Department's general controls over the management, development, and security of its automated information systems.

2. To assess the effectiveness of the Department's internal control over its automated information systems.

Audit Scope

Our audit scope was to examine the information processing and other records of the Department of Education's automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Department's information processing and other records for the period October 1, 1998 through September 30, 2000. Our work was performed between December 1999 and September 2000. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Assessment and Evaluation Phase

   We identified the Department's automated information systems and performed a preliminary assessment of each system to determine those systems with the highest risk. Our risk assessment considered the critical nature of the information processed through each system as well as the number and dollar value of transactions processed. We used this assessment to determine which systems to audit and the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

We reviewed internal control over the Grant Accounting System, Federal Letter of Credit System, J20 System for Food and Nutrition Programs (J20 System), and State Aid Management System (SAMS) pertaining to (a) general controls, which included management and organization controls, system development and documentation controls, program change controls, and local area network controls, and (b) application controls, which included data input, data processing, and data output controls. Specifically, we assessed:

a. Effectiveness of General Controls:

We evaluated Technology Services' management and organization controls, including its information technology policies and procedures and information technology strategic plan; standards and procedures for system development, system documentation, and program change controls; and its information technology security program.

We assessed the system development methodology in place for the development of automated information systems.

We examined system documentation for the Grant Accounting System, Federal Letter of Credit System, J20 System, and SAMS for completeness.

We evaluated the program change control process.

We observed and assessed the controls over the local area network, including physical security, backup, and network access controls.

b. Effectiveness of Internal Control Over Automated Information Systems:

We evaluated controls over access and use of the Grant Accounting System, Federal Letter of Credit System, J20 System, and SAMS.

We assessed and documented internal control over data input, data processing, and data output of the Grant Accounting System, Federal Letter of Credit System, J20 System, and SAMS. We also conducted tests to determine whether the controls were working as intended.

3. Evaluation and Reporting Phase

   We evaluated and reported on the results of the preliminary assessment and evaluation phase and the detailed analysis and testing phase.

Agency Responses and Prior Audit Follow-Up

Our audit report contains 14 findings and 15 corresponding recommendations. The agency preliminary response indicates that the Department agreed with all of the recommendations.

The agency preliminary response which follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Department of Education to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

The Department complied with 2 of the 10 prior audit recommendations included within the scope of our current audit. We repeated 2 prior audit recommendations in this report (Findings 1 and 10) and 6 were rewritten for inclusion in this report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF GENERAL CONTROLS

COMMENT

Background: General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. Although general controls are normally independent of individual computer applications, they provide the framework within which many different applications are processed. Therefore, weaknesses in general controls can adversely affect all of a department's automated information systems.

Audit Objective: To assess the effectiveness of the Department of Education's general controls over the management, development, and security of its automated information systems.

Conclusion: The Department's general controls over the management, development, and security of its automated information systems were limited in their effectiveness and should be improved. Our assessment disclosed two material conditions. The Department had not established a comprehensive information systems security program. Also, the Department had not established effective program change controls.

In addition, we identified reportable conditions related to the effectiveness of information technology, technology services organization and staffing, local area network (LAN) access controls, physical security controls, standardization and documentation of network configuration, system development methodology and system documentation, LAN backup and recovery controls, and business resumption plan.

During the course of our audit, we made several observations that we believe affect the ability of the Department to effectively achieve its information technology (IT) business needs. Specifically, we noted that since fiscal year 1996-97, the Department has had five different chief information officers (CIO) and, at one point, went 18 months without a CIO. The Department had not established a formal selection process to search for and hire the most qualified candidates. Although the five appointed CIOs had management experience, they lacked IT background and experience. The turnover of CIOs and their

inexperience in IT has resulted in ineffective management, planning, and oversight of IT. We also noted that the mission and vision of Technology Services does not specifically address the need to provide IT services to the Department's program areas. We noted a general dissatisfaction among program areas with the quality and timeliness of service provided by Technology Services.

FINDING

1. Comprehensive Information Systems Security Program

The Department had not established a comprehensive information systems security program.

A comprehensive security program should include a comprehensive, periodic risk assessment; resources for independent monitoring of information systems' activity; and detailed policies and procedures for independent safeguarding of all agency information system resources.

The Department had not performed a comprehensive risk assessment. Risk assessments help to identify system risks and appropriate security safeguards. They also help ensure that the computer security systems are cost-effective, up to date, and responsive to threats. Without periodic, comprehensive risk assessments, security risks may go undetected and uncorrected.

The Department had assigned the network security function to the network administrator. Although network administrators have a role to play in maintaining the security of network resources, overall network security should be independent. An independent security officer should monitor system access and educate users about the importance of information systems security. Security officer duties also should include establishing a security program, developing and enforcing security policies and procedures, and monitoring system-recorded security activities and violations.

The Department's lack of a comprehensive security program for safeguarding agency information system resources contributed to the following control weaknesses:

a. The Department had not established effective LAN access controls (Finding 4).

b. The Department should enhance its physical security controls (Finding 5).

c. The Department should improve its LAN backup and recovery controls (Finding 9).

d. The Department had not established effective control procedures to prevent unauthorized access and use of its automated systems (Finding 11).

The Department should include all of its critical information systems in a comprehensive security program. Without a comprehensive security program, management cannot ensure that the Department's controls are operating as intended and that sensitive information will remain confidential.

We reported this condition in two prior audits. The Department indicated that it concurred but could not comply until funds were appropriated for the security officer position.

RECOMMENDATION

WE AGAIN RECOMMEND THAT THE DEPARTMENT ESTABLISH A COMPREHENSIVE INFORMATION SYSTEMS SECURITY PROGRAM.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and informed us that many improvements to security have already been implemented and further improvements will be made. Developing security within cost beneficial parameters is a continuing challenge for any organization.

FINDING

2. Effectiveness of Information Technology (IT)

The Department had not established controls to ensure that IT is used effectively to achieve the Department's business needs. Our review disclosed:

a. The Department had not developed a comprehensive IT strategic plan.

An IT strategic plan provides the framework necessary to help ensure that the Department's automation efforts are directed toward defined and meaningful objectives.

Since fiscal year 1996-97, Technology Services has had five different CIOs. Such turnover in this key management role makes it difficult to create and implement a strategic plan.

Technology Services had been focusing its efforts on the development of the Single Record Student Database and the Michigan Education Information System (MEIS) data warehouse. Other items that should be considered in a more comprehensive IT strategic plan include hardware and software platforms, support of legacy systems*, network strategy, Internet and intranet deployment, and desktop computer strategy.

b. The Department had not established an IT steering committee.

The creation of an IT steering committee, comprised of executive and senior management representing key business units and support functions, is one way of obtaining and involving the appropriate levels of management within the Department.

A key role of an IT steering committee is to direct the IT strategic planning process and ensure a close relationship between the Department and IT planning.

The Department had formed a web steering committee to assist in implementing web-related policy, to provide feedback about the Department's

* *See glossary at end of report for definition.*

web site, and to serve as a forum for web publishers. The Department also established an MEIS data warehouse steering committee to guide the development of the MEIS data warehouse. However, the Department should establish an overall IT steering committee to address broader IT issues.

c. The Department had not conducted a capability maturity model (CMM) assessment.

The framework underlying the CMM applies total quality management practices to software organizations to help them improve their capability to develop high-quality software on schedule and within budget. The CMM guides organizations in steadily improving their capability for developing software.

The Year 2000 Project Office, Department of Management and Budget (DMB), recommended that departments conduct a CMM assessment. Several State departments began using the CMM methodology as a quality assurance measure for their year 2000 software remediation projects. The Department should conduct a CMM assessment and use it to improve the IT organization and software development.

The Department informed us that it has completed some informal assessments of its software maturity level and has completed some steps to get beyond the initial level. However, these assessments have not been documented. The Department informed us that, once it gets the foundation in place for moving to the next level of CMM, it will reassess and document its progress.

Developing a comprehensive IT strategic plan, establishing an IT steering committee, and conducting a CMM assessment would help prioritize and use IT resources in the best manner to support the Department's business needs.

RECOMMENDATION

We recommend that the Department establish controls to ensure that IT is used effectively to achieve the Department's business needs.

AGENCY PRELIMINARY RESPONSE

The Department agreed with this recommendation. In regard to parts a. and b. of this finding, the Department informed us that it has retained the consulting firm of A. J. Boggs and Co. to assist in the development of an IT strategic plan and implementation of an IT steering committee. The first IT steering committee meeting was held on March 8, 2001. A subcommittee was established to develop a strategic plan.

In regard to part c. of the finding, the Department informed us that it has identified the steps that are required to achieve CMM level 2 and will work toward achieving them.

FINDING

3. Technology Services Organization and Staffing

The Department should improve the effectiveness of the Technology Services organization and staffing.

During our audit period, the Department implemented a LAN and converted its legacy systems from the mainframe to the LAN. In addition, the Department began developing web-based systems on the LAN. These technology changes have resulted in the use of new operating systems, programming languages, and database software. The shift in technology from mainframe to LAN has resulted in the need for different skills among Technology Services staff.

Our review of Technology Services staffing disclosed:

a. Technology Services did not employ staff proficient in the programming language needed to maintain four of the Department's critical systems that we reviewed. Some of these systems will require enhancements every year to comply with changes in federal and State regulations. In order to effectively maintain these systems, Technology Services should develop alternatives to obtain the expertise to support the Department's critical systems. Alternatives could include hiring additional staff, contracting with a software development firm, or training current staff.

b. Technology Services did not have sufficient staff to program its web-based systems on a timely basis. Owners of the web-based systems indicated dissatisfaction with the time it took to implement the systems. Because of the numerous systems under development and because of other job responsibilities, web development was not done on a timely basis and in accordance with sound development practices (Findings 7 and 8). For example, in November 1999, the Office of School Support Services requested that Technology Services develop web-based input screens for the J20 System for Food and Nutrition Programs (J20 System) by September 2000 for school districts to input their school lunch program applications. However, the screens have not been implemented, resulting in the Office of School Support Services having to input the applications for the school districts. The untimely development of the web-based system also resulted in the continued use of the mainframe computer system, which is inefficient and has caused problems with payments. In another instance, programs were not properly tested and implemented using a sound change control process. This resulted in a loss of data.

Technology Services had prepared professional development plans for each Technology Services staff member and had begun sending staff to training classes. Technology Services also identified the areas in which it was lacking skilled employees. However, Technology Services recognizes the difficulty in changing skills to meet new technology. It will take time for employees to acquire and apply new skills.

RECOMMENDATION

We recommend that the Department improve the effectiveness of the Technology Services organization and staffing.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and informed us that it will continue to aggressively train existing staff.

FINDING

4. LAN Access Controls

The Department had not established effective LAN access controls.

Effective LAN access controls require users to be uniquely identified and authenticated through the use of a usercode and password. Effective controls also include granting access to data, program, and system files only to the extent necessary for individuals to perform their assigned duties. Our review of access controls at the network level disclosed:

a. The Department did not disable the usercodes of employees and contractors who had terminated employment or had transferred to another department. We identified usercodes of 19 employees and two contractors that should have been disabled. Allowing usercodes of former employees to remain active increases the risk of unauthorized changes to the LAN and automated systems.

   The Department informed us that it is working on a process to improve communication between Human Resource Services and Technology Services to ensure the timely notification of employee termination dates.

   We reported this condition in our prior audit as it related to mainframe computer usercodes. The Department agreed and indicated that staff would work with Human Resource Services to identify terminated employees and remove their access to computer systems.

b. The Department did not establish and enforce sound password rules over network passwords. To help prevent the compromise of usercodes and passwords, all usercodes should have an associated password and the reuse of previous passwords should be prohibited.

c. The Department did not require users to periodically change their network passwords. DMB Administrative Guide procedure 1310.02 requires that passwords be changed periodically. Changing passwords on a regular basis helps ensure password confidentiality and reduces the risk of unauthorized access to the system.

d. The Department had not established procedures for adding and removing users from the network. The Department should implement the use of a form, signed by an employee's supervisor, to establish or remove a usercode on the LAN. This form would provide the authorization for a user to have access to a system and also document the access rights that should be granted to a user.

e. The Department did not automatically disconnect computer workstations or use password-protected screen savers after a reasonable period of inactivity. This could result in unauthorized system access if a workstation is left unattended. DMB Administrative Guide procedure 1310.02 requires that workstations automatically log off if left unattended for a specific period of time.

   We reported this condition in our prior audit as it related to disconnecting mainframe terminals. The Department agreed with the finding but informed us that it could not comply with the recommendation because of limitations in the operating system software.

f. The Department did not activate the audit log feature to monitor sensitive network activity, such as granting administrator rights, the use of administrator commands, and changes to server configuration. An audit log records the activity performed by specific users. For example, network administrators perform and manage sensitive network activity that could be recorded in the audit log. The Department should identify sensitive activity and develop methods to monitor it.

RECOMMENDATION

We recommend that the Department establish effective LAN access controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and informed us that it is implementing a phased plan to establish better network password control. The Department informed us that it now requires periodic password changes and password uniqueness.

FINDING

5. Physical Security Controls

The Department should enhance its physical security controls.

Effective physical security controls would help ensure that the LAN and LAN hardware are safeguarded and that access is limited to individuals responsible for

managing the LAN. Our review of physical security controls identified the following:

a. Access to the file server room was controlled by a combination keypad; however, the Department was unable to provide us with a list of all individuals who knew the combination for the keypad. In addition, another State agency stored network resources in the Department's file server room. The Department did not have control over who had access to the file server room from the other agency. The Department should establish a list of authorized users and periodically change the keypad combination to reduce the likelihood of unauthorized access. Further, the Department should assess the risk of other State agency staff having access to the file server room.

b. The Department did not store LAN hardware in a separate and secure location. The Department's file server room, which contained LAN hardware, was also the workspace for some Technology Services staff and student interns. In addition, another State agency had office space adjacent to the file server room. Access to the file server room could be gained through the partial wall that separates these two rooms. The Department should formally request that DMB modify the partial wall to improve the security of network resources.

c. The Department did not maintain a log of visitors to the file server room. Maintaining a visitor log would help the Department identify who was in the file server room in the event of a questionable action occurring to the LAN.

RECOMMENDATION

We recommend that the Department enhance its physical security controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and informed us that it has complied. The Department installed locked server cabinets with a limited number of people having keys to these cabinets.

FINDING

6. Standardization and Documentation of Network Configuration

The Department should continue its efforts to standardize and document network configuration.

The Department did not define and document standards and procedures to ensure the consistency of workstation, server, and operating system configuration; document procedures to identify, report, and track network problems; and maintain documentation and schematics describing how the network was designed and implemented. If the Department had established and followed standards for network configuration, the Department's network might have been implemented in a more effective manner. For example, because of the way that traffic was routed, network performance was slow and not optimized.

The lack of standards and procedures could adversely affect the ability of the Department to maintain and operate the network. Establishing and documenting network standards and procedures would help ensure the standard configuration, operation, and administration of the network.

When the LAN was first implemented, the Department did not have staff experienced in LAN administration. As a result, the LAN was not effectively implemented. In 1999, the Department hired a new LAN administrator who has taken steps to improve the security and design of the LAN.

RECOMMENDATION

We recommend that the Department continue its efforts to standardize and document network configuration.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and will comply.

FINDING

7. System Development Methodology and System Documentation

The Department had not established and implemented a system development methodology to be followed when systems are being designed, developed, and maintained. In addition, the Department had not developed complete system

documentation for the Grant Accounting System, Federal Letter of Credit System, J20 System, and State Aid Management System (SAMS). Our review disclosed:

a. DMB Administrative Guide procedure 1310.06 requires that agencies adopt the use of a system development life cycle (SDLC) methodology addressing the entire scope of an IT project, including project definition, design, development, installation, and postimplementation review. Using an SDLC will help ensure the development of systems that meet the needs of their users. It will also help ensure that systems are implemented on time and within budget.

   We noted that the Grant Accounting System, Federal Letter of Credit System, and J20 System were not developed using an SDLC. Specifically, the Department had not sufficiently conducted project definition, system design, system testing, and postimplementation reviews. As a result, the Department continues to make numerous changes to the Grant Accounting System to fix problems that may have been avoided if adequate development and testing had been done. Also, as a result of not completing system analysis and design of the J20 System, the Department had to discard work done by the system development contractor and redevelop the system.

   During our audit, Technology Services informed us that it had established an SDLC methodology. However, it needs to distribute the methodology throughout the Department to ensure that all developers properly develop applications.

b. DMB Administrative Guide procedure 1310.07 defines the documentation that should be produced at each phase of development. System documentation helps promote operating efficiencies, minimizes the impact of employee turnover, and reduces the amount of resources needed to maintain programs.

   The Department had file layouts, source code listings, and, for SAMS, documentation of yearly changes to the State School Aid Act. However, other common system documentation had not been prepared. We noted that none of the four systems we reviewed had the following documentation, which is required by procedure 1310.07: definition of user requirements; detailed design documents, including functional and technical specifications; program specifications; test documentation; conversion plans; and user procedures.

We reported this condition in our prior audit as it related to test documentation on mainframe computer systems. The Department indicated that test documentation was not always available because of decreasing staff levels.

RECOMMENDATIONS

We recommend that the Department continue its efforts to establish and implement a system development methodology to be followed when systems are being designed, developed, and maintained.

We also recommend that the Department develop complete system documentation for the Grant Accounting System, Federal Letter of Credit System, J20 System, and SAMS.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendations and will continue its efforts to establish a system development methodology. In addition, the Department informed us that it has taken the following steps: purchase of Rational Unified Process, which is a methodology and software lifecycle documentation process that implements industry standard best practices; purchase of Rational Rose visual modeling and analysis and design tool for documenting the requirements for analysis and design of a system; implementation of a software development service request form; and implementation of Microsoft Project 2000, a project planning tool.

FINDING

8. Program Change Controls

The Department had not established effective program change controls.

Establishing controls over the modification of application software programs helps ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help ensure all programs and program modifications are properly authorized, tested, and approved and that access to programs and movement of programs to production is carefully controlled.

Our review of program change controls disclosed:

a. The Department had not established program libraries for application programs. Using separate libraries for development, test, and production programs would help ensure the security and integrity of programs. In addition, programs maintained in libraries can be labeled, dated, and inventoried in a way that diminishes the risk that programs will be lost or misidentified.

b. The Department did not control the movement of computer programs into production. To ensure the integrity of changes to programs, the Department should implement a process that segregates the duties of making changes to programs and moving the programs into production. The ability to move changes into production should be the responsibility of a library control group. Allowing programmers to move programs into production increases the risk that unauthorized changes could be made to the programs.

   We reported this condition in our prior audit as it related to program changes on mainframe computer systems. The Department agreed with the finding but indicated that staff reductions made it not possible to implement a process.

c. The Department did not document and maintain all requests for program changes. The Department should develop a change request form to document change requests and approvals. The use of a standardized form helps ensure that all requests are clearly communicated and that approvals are documented.

d. The Department did not maintain previous versions of application programs. Maintaining versions of programs is important in the event that a program needs to be restored because of errors in the current version. Maintaining versions is also important in proving the processing procedures that were followed at the time. For the Grant Accounting and Federal Letter of Credit Systems, when the Department moves a modified program into production, it writes over the old program. For the J20 System, the Department maintains only the current and most recent version. Without maintaining previous program versions that can serve as an audit trail, the Department cannot re-create a previous version of the program and the program's history.

Version control software can be acquired for client-server systems that would establish program libraries, control the movement of programs into production, maintain a record of program changes, and maintain versions of programs. The Department should determine the feasibility of obtaining version control software.

RECOMMENDATION

We recommend that the Department establish effective program change controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and informed us that it is in the process of establishing effective program change controls. The Department is implementing Microsoft SourceSafe configuration management and version control software and informed us that it has sent one staff person to training in the administration of the software. The implementation of the configuration management software and methods is planned in the immediate future.

FINDING

9. LAN Backup and Recovery Controls

The Department should improve its LAN backup and recovery controls.

Effective LAN backup and recovery controls ensure that LAN applications can be restored in the event of a disaster. Our review of backup and recovery controls over the LAN disclosed:

a. The Department did not store current copies of its LAN daily backup files off site. The Department stored its daily backup files on site for up to two weeks before moving them off site. In the event of a fire or other disaster, up to two weeks of data could be lost.

b. The Department's off-site facility for storing backup files did not meet DMB guidelines. DMB Administrative Guide procedure 1310.02 requires that an off-site backup file library or vault be utilized that is a minimum of five miles from the main processing site. The Department's off-site storage facility was in an adjacent building.

c. The Department's written backup procedures were not complete. The backup procedures did not address the roles and responsibilities of staff, procedures that Technology Services should follow in backing up data, and procedures that Technology Services should follow when restoring files from the backup tapes.

   The Department informed us that it had a process to address these areas; however, it was not in writing.

RECOMMENDATION

We recommend that the Department improve its LAN backup and recovery controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and will comply. In regard to part a. of the finding, the Department informed us that it will study the timing of off-site backup rotation. In regard to part b. of the finding, the Department informed us that it will begin using a new off-site storage location. In regard to part c. of the finding, the Department is in the process of developing written backup procedures.

FINDING

10. Business Resumption Plan

The Department had not developed a comprehensive business resumption plan.

A business resumption plan provides for continued operations in the event of a disaster. The business resumption plan should contain an updated and detailed description of all strategies, standards, procedures, schedules, and resources required to complete the business resumption process.

The Department had not:

a. Identified its critical systems and the amount of time that the Department can be without the systems.

b. Completed a risk analysis to assess the risk of a prolonged service outage.

c. Documented the business resumption plan, identified the participants in the plan, and established the roles and responsibilities of the plan participants.

d. Thoroughly tested the business resumption plan and documented any testing that it had performed.

Completion of a business resumption plan may help the Department ensure timely resumption of operations and recovery of data in the event of a disaster.

We reported this condition in two prior audits. The Department agreed with the recommendation but had not complied. The Department indicated that it had been involved with a DMB-sponsored initiative to establish standard procedures for all State departments. However, the initiative ended when key DMB staff retired.

RECOMMENDATION

WE AGAIN RECOMMEND THAT THE DEPARTMENT DEVELOP A COMPREHENSIVE BUSINESS RESUMPTION PLAN.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation but informed us that it lacks the financial and human resources to comply with it. The Department will, however, continually strive to comply.

EFFECTIVENESS OF INTERNAL CONTROL OVER AUTOMATED INFORMATION SYSTEMS

COMMENT

Audit Objective: To assess the effectiveness of the Department's internal control over its automated information systems.

Conclusion: The Department's internal control over its automated information systems was generally effective. We determined that data was accurately processed by the automated information systems and that, in general, payments were properly calculated and paid to the recipients. However, we identified reportable conditions

regarding system access controls, SAMS processing controls, completeness and accuracy of processing, and audit trails.

Noteworthy Accomplishments: We conducted a survey of a sample of school districts to obtain their opinions about the Grant Accounting System, J20 System, and SAMS. The survey disclosed that the school districts were generally satisfied with the systems. The survey also disclosed that the school districts were very satisfied with the timeliness in which payments were received.

FINDING

11. System Access Controls

The Department had not established effective control procedures to prevent unauthorized access and use of its automated systems.

Effective control procedures help ensure that only authorized users access or change data and program files. In addition to the four systems included in our audit, we also reviewed usercode and password security over the Education Data Network and the K-12 Database. Our review disclosed:

a. The Department did not restrict access to data and program files to only authorized users. We noted:

(1) The Department did not properly assign access rights to the 6 systems we reviewed. We identified 21 users with full access rights. These users should have been restricted to read-only access or other limited rights based on job responsibilities. The Department should assess the users' access needs and adjust their access rights accordingly.

(2) The Department did not restrict access to SAMS software and data files. All Department employees had read access to these files. Access to these files should be restricted to State Aid and School Financial Services (SASFS) staff only.

The Department immediately corrected this weakness after we brought it to its attention.

(3) The Department gave programmers access to production data for 4 of the systems we reviewed. Sound internal control requires that production data be accessed and changed only by authorized users and that programmers access only test data. Restricting access to production data or establishing compensating controls will help ensure the integrity of the data.

We reported this condition in two prior audits as it related to production data on the mainframe computer. The Department agreed with the finding but had not complied.

b. The Department did not prevent the sharing of usercodes and passwords. The database administrator for the K-12 Database shared his usercode and password with Technology Services staff. The use of unique usercodes would allow management to identify the originators of transactions and help to ensure that unauthorized personnel do not have access to data.

RECOMMENDATION

We recommend that the Department establish effective control procedures to prevent unauthorized access and use of its automated systems.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and will comply.

FINDING

12. SAMS Processing Controls

The Department had not completely implemented controls over the processing of State aid payments. Our review disclosed:

a. The Department did not have automated controls to ensure the accuracy of SAMS processing.

SASFS staff informed us that SAMS programs have mistakenly been processed out of sequence, resulting in the need to rerun programs. Running programs out of sequence could result in the incorrect calculation of State aid payments. Since our prior financial audit of the School Aid Fund, SASFS

implemented a new manual process to prevent the improper sequence of programs. However, SAMS did not automatically alert the user when this sequence was not followed.

Establishing automated controls over the sequence of programs would help ensure the accuracy of State aid payments.

We also reported this condition in prior financial audits of the School Aid Fund.

b. The Department had not established system access rights to control the calculation and certification of State aid payments.

Each month, SASFS calculates and certifies the monthly State aid payment. The ability to calculate the payment should be restricted to designated SASFS staff. The ability to certify the payment should be restricted to SASFS managers.

During the period October 1998 through May 2000, we identified:

(1) Fifty-four instances in which programmers performed calculations.

(2) Twenty-five instances in which programmers performed certifications.

(3) Ninety-two instances in which SASFS staff performed certifications.

Although we identified these instances of inappropriate calculations and certifications, the Department informed us that it believes that the overall certification of the payments was done by the SASFS manager.

c. The Department had not developed user-management capability within SAMS. Developing a user-management screen would allow a manager within SASFS to add and remove users from SAMS. Because this capability has not been developed, a programmer must modify program code to add or remove a user. Use of a user-management screen by the SASFS manager would be a more appropriate method of adding and removing users.

The Department should develop and implement access rights to restrict the abilities of staff and programmers.

RECOMMENDATION

We recommend that the Department completely implement controls over the processing of State aid payments.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and will comply. In regard to part a. of the finding, the Department agreed that computer program controls will provide an additional safeguard and informed us that it will implement them as soon as resources are available. In regard to part b. of the finding, the Department informed us that programmers executed the calculation and certification programs on a limited basis in order to identify errors. In addition, the Department informed us that the payment manager usually certifies each calculation or can designate another employee to certify the calculations. The Department will define the procedures for this in writing. In regard to part c. of the finding, the Department agreed that user controls require additional programming; however, other mission critical programming changes have taken precedence.

FINDING

13. Completeness and Accuracy of Processing

The Department had not established effective and efficient controls to ensure the completeness and accuracy of processing. Our review disclosed:

a. The Department had not established a process to ensure the completeness of data imported to SAMS. SAMS receives school membership data from the Department's K-12 Database. Establishing a process such as the reconciliation of control totals would help ensure that all records are received during the import process.

   The Department informed us that it had tested control totals for the import of membership data to the K-12 Database; however, totals were not reviewed for each import process.

b. The Department had not established a process to ensure the propriety of files being processed by the Grant Accounting System. The Grant Accounting System receives a weekly file from the J20 System to process school lunch reimbursement payments. However, the Department did not design the Grant Accounting System to automatically check the date of the file to ensure that the proper file is being processed. This resulted in a duplicate school lunch payment being made to approximately 360 recipients.

c. The Department had not established an efficient method for the Office of School Support Services to verify that the payment data sent from the J20 System to the Grant Accounting System was completely and accurately processed. The previous Grant Accounting System created a report of the amounts that were sent and received. The feature is not functioning in the new Grant Accounting System. As a result, the Office of School Support Services manually compares two lengthy reports to check the accuracy of payments made to each school district. Implementing automated processing control totals would be a more efficient method to ensure the completeness and accuracy of payments.

RECOMMENDATION

We recommend that the Department establish effective and efficient controls to ensure the completeness and accuracy of processing.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and will comply.

FINDING

14. Audit Trails

The Department had not established system audit trails for the identification of transactions and the reconstruction of data files.

The Department did not record complete identifying information about changes to data on the Education Data Network and the K-12 Database. Data recorded on these systems includes full-time equivalent State aid counts, pupil headcounts, staff counts, and financial data.

Audit trails should be developed to provide a history of changes to the data, including the user who made the change, the date and time of the change, and a before and after image of the data. Without an audit trail, it is difficult to prove accountability for transactions and to ensure the reliability and accuracy of payments to school districts.

RECOMMENDATION

We recommend that the Department establish system audit trails for the identification of transactions and the reconstruction of data files.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the recommendation and informed us that it will comply in any new systems development.

Glossary of Acronyms and Terms

categorical programs	The various special program grants that are designated in the State School Aid Act. Examples of categorical programs include: at-risk pupils, special education, vocational education, and adult education.
CIO	chief information officer.
client-server	An architecture in which one computer can get information from another. The client is the computer that asks for access to data, software, or services. The server, which can be anything from a personal computer to a mainframe, supplies the requested data or services for the client.
CMM	capability maturity model.
DMB	Department of Management and Budget.
Education Data Network	A system for the electronic collection of data from school districts using an Internet connection.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical for the amount of resources applied or minimizing the amount of resources required to attain a certain level of outputs or outcomes.
foundation allowance	The guaranteed minimum amount paid to each school district for each reported pupil. Foundation allowance funds are to be used for the general operating expenses of a school district. The starting point for the foundation allowance is the eligible base revenue each school district received per pupil in the 1993-94 school year. This amount

	is then increased each year by an amount specified in the annual amendments to the State School Aid Act.
internal control	The management control environment, management information system, and control policies and procedures established by management to provide reasonable assurance that goals are met; that resources are used in compliance with laws and regulations; and that valid and reliable performance related information is obtained and reported.
IT	information technology.
J20 System	J20 System for Food and Nutrition Programs.
K-12 Database	A computer database that contains the following information: achievement data, adult education, compensatory education, financial data, food and nutrition, full-time equivalent State aid counts, pupil headcounts, instruction data, school code master, special education, staff counts, State aid system, and transportation data.
legacy system	An information system that has been in use for a long time, usually on a mainframe computer or a minicomputer.
local area network (LAN)	A series of interconnected computers, printers, and other computer equipment that share hardware and software resources. The service area is usually limited to a given floor, office area, or building.
Management Information Database (MIDB)	A facility that replicates and brings together into one logical system an organization's diverse data. The facility's primary function is to serve as a database for data inquiry and reporting uses only. Historical information from the State's accounting, purchasing, personnel, and payroll information systems are also in the database.

material condition	A serious reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the opinion of an interested person concerning the effectiveness and efficiency of the program.
Michigan Administrative Information Network (MAIN)	A fully integrated automated financial management system for the State of Michigan.
Michigan Education Information System (MEIS)	A web-based system used for electronic collection of data from school districts.
mission	The agency's main purpose or the reason that the agency was established.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
reportable condition	A matter coming to the auditor's attention that, in the auditor's judgment, should be communicated because it represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
SAMS	State Aid Management System.
SASFS	Office of State Aid and School Financial Services.
SDLC	system development life cycle.