A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit

Arizona Department of Education—

Information Management

AUGUST • 2006
REPORT NO. 06 – 07

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Representative **Laura Knaperek,** Chair

Representative **Tom Boone**
Representative **Ted Downing**
Representative **Pete Rios**
Representative **Steve Yarbrough**
Representative **Jim Weiers** *(ex-officio)*

Senator **Robert Blendu,** Vice Chair

Senator **Ed Ableser**
Senator **Carolyn Allen**
Senator **John Huppenthal**
Senator **Richard Miranda**
Senator **Ken Bennett** *(ex-officio)*

Audit Staff

Melanie M. Chesney, Director
Joseph D. Moore, ITS Director and Contact Person

Dot Reinhard, Manager
Estella Arredondo
Allan Friedman
Jenner Holden
Emily Chipman
Melynda Harris
Thomas Huber

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:
www.azauditor.gov

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

August 17, 2006

Members of the Arizona Legislature

The Honorable Janet Napolitano, Governor

Mr. Tom Horne, State Superintendent of Public Instruction
Arizona Department of Education

Transmitted herewith is a report of the Auditor General, A Performance Audit of the Arizona Department of Education—Information Management. This report is in response to Arizona Revised Statutes (A.R.S.) §41-2958 and was conducted under the authority vested in the Auditor General by A.R.S. §41-1279.03. I am also transmitting with this report a copy of the Report Highlights for this audit to provide a quick summary for your convenience.

As outlined in its response, the Department of Education agrees with all but one of the findings and plans to implement all but one of the recommendations.

My staff and I will be pleased to discuss or clarify items in the report.

This report will be released to the public on August 18, 2006.

Sincerely,

Debbie Davenport
Auditor General

Enclosure

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

SUMMARY

The Office of the Auditor General has conducted a performance audit of the Arizona Department of Education's (ADE) information management function pursuant to Arizona Revised Statutes (A.R.S.) §41-2958. This audit was conducted under the authority vested in the Auditor General by A.R.S. §41-1279.03 and is the third in a series of three reports regarding ADE. The other two audit reports address aspects of ADE's administration and allocation of funds and its accountability programs.

Background

ADE depends on information technology (IT) to manage its own operations and to provide state-wide oversight and assistance to Arizona's 238 school districts and 487 charter schools. IT is important to ADE's processes for calculating and administering the transfer of approximately $3 billion in state appropriations to districts and charter schools. It is also important for state-wide reporting on education initiatives such as AZ LEARNS and No Child Left Behind (NCLB). Many different groups rely on ADE's IT resources, including parents, teachers, schools, and the Legislature for various purposes such as obtaining tutoring information, applying for teaching certificates and positions, or obtaining information about Arizona's schools, their students, and their finances. At the heart of ADE's technology efforts is its Student Accountability Information System (SAIS). SAIS was established by statute to enable school districts and charter schools to transmit student-level data and school finance data electronically through the Internet to ADE to comply with ADE's and the State Board of Education's statutory obligations.

ADE needs to better manage security of its information technology systems and operations (see pages 9 through 16)

Sensitive information, such as social security numbers, has been exposed because of security weaknesses in ADE's Web-based applications. However, auditors found no indication that the security weaknesses identified have yet been exploited or that sensitive information has been compromised.

The Auditor General hired an independent consulting firm to help its auditors assess 12 of ADE's 76 Web-based applications. These 12 applications are among the most frequently used and/or contain the most sensitive data. The auditors found 8 different types of critical vulnerabilities. Most of the applications had 5 or more of these vulnerabilities.

These weaknesses could potentially:

- Enable an attacker to obtain access to other users' accounts, view sensitive information, or perform functions they are not authorized to; or
- Provide attackers with useful information that could assist them in carrying out further attacks.

In response to the Web-based application vulnerabilities found in this audit, ADE began to take steps to identify critical applications and prioritize actions needed to assess and correct discovered vulnerabilities. ADE management asserts those activities were performed during May and June 2006.

However, the vulnerabilities in ADE's applications are only part of the overall security weaknesses in ADE's IT operations. While ADE has policies and procedures in place for many important security objectives, auditors found that for 12 of 13 areas reviewed, these policies and procedures were either inadequate or ineffective, including those over such functions as:

- Password management;
- Installing security updates for their IT systems; and
- Monitoring systems to detect attacks and/or identify unauthorized uses.

Although previous security assessments have alerted ADE to many security concerns, it has not always taken sufficient action to address them. For example, while ADE did fix some specific Web-based application weaknesses found in a 2004 security assessment of its systems, other weaknesses noted in the reports were not addressed. Several of these weaknesses were serious in nature and should have been addressed immediately.

ADE has indicated that it has not had a coordinated approach for addressing security concerns that it identifies or that come to its attention. ADE should consider creating an appropriate position to be responsible for all IT security within ADE. The reporting line of the security position should be such that it can effectively design, implement, and enforce compliance with the organization's security policies, standards, and procedures, and ensure that they are functioning effectively.

ADE can further enhance SAIS' reliability (see pages 17 through 28)

As the primary entity responsible for operating and maintaining SAIS, ADE plays an important role in helping ensure SAIS' reliability. SAIS was established by statute to enable school districts and charter schools to electronically transmit student-level data and school finance data to ADE. According to a survey conducted by this Office, although the majority of SAIS users have confidence in the accuracy of SAIS data, some users continue to have concerns. Approximately 29 percent of SAIS users who auditors surveyed reported that they were not confident that the data in SAIS was accurate when it was needed for final reporting or funding purposes, and in 2005 the Arizona School Administrators adopted a formal position that data within SAIS is unreliable. ADE can further improve the reliability and processing performance of SAIS by (1) adding more controls such as data variance checks to ensure reliability; (2) taking steps to improve functionality such as providing the capability to archive reports; and (3) monitoring the performance of and potentially rating the various software packages that districts and schools use to submit data to SAIS.

ADE has established some data validation controls, and improving these controls would help further ensure data accuracy. Input controls are designed to help ensure that the data entered into SAIS is accurate. Although some input controls are in place, ADE should add another type, known as variance checks. Variance checks would alert ADE to unusual changes in the data such as a large change in the number of students from the prior year. ADE also needs to add automated process controls to SAIS. Process controls are designed to ensure that no data is added, lost, or altered during processing. Adding some process controls, such as data reconciliation at key points in the processing of SAIS data, would also help enhance data accuracy.

ADE can also take some basic steps to improve SAIS' functioning. For example, ADE should continue its efforts to establish the ability to archive SAIS reports so that users will have access to historical report data. ADE should also establish a tactical team comprising internal and external stakeholders to identify and prioritize other changes to SAIS that can address users' concerns.

Finally, ADE also needs to improve its oversight of the software packages that SAIS users use to transmit data to SAIS. School districts and charter schools develop or buy student management system (SMS) software packages to electronically submit data to SAIS. There are at least 20 different packages in use. Auditors found that the quality of these packages varies considerably. Based on information provided by ADE, one software package had errors in only 0.7 percent of the data submitted, while another package had a 31.8 percent error rate. There are several reasons the software quality varies, including ADE's relaxation of testing requirements. According

to ADE, resource limitations have prevented it from continuing its original vendor testing requirements. However, to further enhance SAIS data reliability, ADE should take action to enhance SMS software performance by monitoring it and should consider rating or certifying SMS software packages based on performance.

ADE needs to improve IT project management and operations oversight (see pages 29 through 34)

ADE needs to improve its approach for managing systems development projects and for overseeing its IT operations. The ADE IT section, which currently has 57 positions, is primarily responsible for maintaining all of ADE's information technology resources and for managing ADE's internal and external networks. There is a lack of consistency in how systems are developed—both by the IT section and by other units within ADE—and many systems have not been developed following a standard agency-wide development process. Many of ADE's information systems lack good documentation, which has caused difficulties in maintaining and modifying the systems. ADE needs to ensure that systems development projects follow a standard approach and are well documented. ADE also needs to ensure that this standard approach applies to all of ADE's projects, whether developed by the IT section or by other ADE units.

The IT section should also improve key IT oversight operations. It should develop performance indicators, conduct risk assessments of threats to its operations, and prepare an adequate business continuity plan.

ADE needs to ensure its information technology meets its business needs (see pages 35 through 39)

Although IT is key to many of ADE's administrative functions and responsibilities, ADE has not adequately ensured that its IT resources meet its business needs. Specifically, IT management or staff do not adequately participate in developing ADE's strategic plan, despite the fact that IT resources may be needed to ensure that objectives are met. ADE also lacks a department-wide process for prioritizing IT projects. ADE needs to take at least two steps to ensure that IT can effectively support its business goals and objectives, including:

- Establishing an IT steering committee. The committee should include representatives from senior management, user management, and the IT function. Once established, the committee should be responsible for things such as ensuring adequate IT involvement in the department and division

planning processes, providing overall IT direction, and ensuring that adequate processes exist for identifying, funding, and allocating department-wide IT resource costs.

- Considering whether the IT section's placement within the organization adequately ensures that IT can effectively meet ADE's business goals and objectives.

In addition, the IT section's internal planning process is limited and does not identify the resources it needs to maintain and operate its current systems or plan for future IT initiatives. Therefore, ADE should ensure that the IT section establishes an effective planning process. This process should include developing a strategic plan with input from key stakeholders that defines long-term direction, and developing an action plan that, among other things, formulates strategies; evaluates costs, benefits, and possible consequences of alternative courses of action; assigns responsibility for implementation; and determines the resources necessary to carry out the plan.

ADE not in full compliance with student-level data collection notification and disposal requirements (see pages 41 through 42)

ADE is not complying with two data-related statutory requirements. ADE has not complied with a requirement that it tell school districts and charter schools the specific statutory authority for each item of student-related data that it requires them to submit. However, ADE has begun to compile this information and hopes to publish it by the middle of fiscal year 2007.

ADE has also not complied with a requirement that it adopt guidelines to remove outdated student information from SAIS. ADE explains that it has not adopted guidelines due to state and federal initiatives that suggest ADE may need to retain education data for longer periods than statute currently calls for. However, it appears that statute does not prescribe a retention period for student-level data. Therefore, ADE should adopt a retention schedule for such data and adopt guidelines to remove the outdated data in SAIS in accordance with state statute.

TABLE OF CONTENTS

◆ continued

TABLE OF CONTENTS

concluded ◆

INTRODUCTION & BACKGROUND

The Office of the Auditor General has conducted a performance audit of the Arizona Department of Education's (ADE) information management function pursuant to Arizona Revised Statutes (A.R.S.) §41-2958. This audit was conducted under the authority vested in the Auditor General by A.R.S. §41-1279.03 and is the third in a series of three reports regarding ADE. The other two audit reports address aspects of ADE's administration and allocation of funds and its accountability programs.

ADE is highly dependent on information technology

ADE is highly dependent on the use of information technology (IT). IT is critical to ADE's ability to manage its own operations and to provide state-wide oversight and assistance to Arizona's 238 school districts and 487 charter schools. For example, IT is important to ADE's processes for calculating and administering the transfer of approximately $3 billion in state appropriations to districts and charter schools, and for state-wide reporting on education initiatives and mandates such as AZ LEARNS,[1] Arizona's Instrument to Measure Standards (AIMS), and the federal No Child Left Behind (NCLB) requirements.[1—3]

IT is critical to ADE's own operations and oversight of and assistance to Arizona's public education programs.

ADE operates its own internal computer network and has developed and maintains a number of computer systems to meet its business needs. These systems are used to perform a variety of functions, including the management and tracking of the expenditure of state and federal funds for the programs it administers, and the collection and reporting of information about students, teachers, and schools in Arizona. Many of these systems are accessible over the Internet.

Many different groups rely on ADE's IT resources. ADE staff relies on its systems to carry out many of their day-to-day responsibilities. Members of the public, including

1 AZ LEARNS is ADE's school accountability system that it also uses to meet NCLB's accountability requirements.

2 AIMS is a standards-based test given to students in Arizona. Effective for the graduating class of 2006, high school students are required to pass AIMS tests in order to graduate. AIMS is used to help measure students' progress toward mastering reading, writing, and mathematics standards that the Arizona Board of Education established.

3 NCLB was signed into law in January 2002. Under the act's accountability provisions, states must describe how they will close the achievement gap between students and make sure all students, including those who are disadvantaged, achieve academic proficiency. States must produce annual report cards to inform parents and communities about state and school progress.

parents and students, may use ADE's Web site to obtain school information, such as school report cards, and AIMS information, such as requirements, study guides, tutoring information, and school or district test results. Teachers may use the Web site to obtain information about educational standards, curriculum development resources, and study guides for AIMS tests, and to apply for teaching certificates or teaching positions throughout the State. Districts, schools, and charter schools use ADE's Student Accountability Information System (SAIS) to submit electronic information, such as district and school identification codes, and students' names, birthdates, identification numbers, absences, and special education enrollment information to ADE. Policymakers, such as the Legislature, also rely on ADE's ability to provide information from their systems about Arizona's schools, their students, and their finances.

ADE's IT systems need to be secure and produce accurate and complete information in a timely manner.

Because so many individuals and groups rely on ADE's IT resources, and because of the quantity and type of information that ADE maintains on its systems, it is especially important that ADE's systems be secure and that they produce accurate and complete information in a timely manner. Security is particularly important because of the sensitive nature of some of the information that ADE maintains on its systems, such as students' names, birthdates, and attendance records, and teachers' names and social security numbers. Additionally, given ADE's dependence on IT, it must ensure that its IT resources are developed and maintained appropriately, operated effectively, available when needed, and meet its business needs.

SAIS a key component of ADE's IT operations

SAIS is a key component of ADE's technology efforts. SAIS was established by statute to enable school districts and charter schools to transmit student-level data and school finance data electronically through the Internet to ADE for the purposes of complying with the statutory obligations of ADE and the State Board of Education. Districts and charter schools are required by statute to submit electronic data on a school-by-school basis, including student-level data, to ADE so that they can receive monies for the cost of educating students. Districts and charter schools were originally required to begin submitting this data to ADE by July 1, 2001. However, according to agency officials, the system did not become fully functional until the 2002-2003 school year. SAIS is used as the basis for calculating Average Daily Membership (ADM) and distributing about $3 billion in state appropriations to districts and charter schools.[1] Funding for school districts is based on prior year student attendance data with some adjustments made for certain exceptions, such as high-growth school districts. Funding for charter schools is based on current year attendance data.

[1] ADM is defined in A.R.S. §15-901 and is the total enrollment of fractional (i.e. less than full-time) and full-time students, minus withdrawals, of each school day through the first 100 days or 200 days in session, as applicable, for the current year.

SAIS' operation involves significant electronic data processing as well as manual effort for both SAIS users and at ADE. Information entered into SAIS is initially recorded in individual SAIS users' data systems, referred to as Student Management Systems (SMS). According to agency information, at least 20 different SMS software packages, developed either by districts or purchased from outside vendors, are used to collect and transmit student data to SAIS. SAIS users are not required to submit information to ADE more often than once every 20 school days. The information must be sent in specific formats, which ADE defines. SAIS users upload their information on the Internet to ADE, where it is then added into the SAIS databases. SAIS receives, validates, and processes the data required by statute to be submitted by Arizona's districts and charter schools. In fiscal year 2006, approximately 46.5 million student data transactions were submitted, such as records of student attendance or absence from school, addition of new students, changes in student schools, etc.

In fiscal year 2006, SAIS processed approximately 46.5 million student data transactions.

Between fiscal years 1997 and 2006, ADE reports spending approximately $11 million for costs associated with SAIS' development and maintenance. In addition, ADE provided about 90 percent of the $4.5 million it received through Proposition 301 in fiscal year 2002 to districts and charter schools to help them develop system interfaces.

IT section

ADE has an IT section that reports to the Associate Superintendent for Education Policy. This section is primarily responsible for maintaining all of ADE's information technology resources and for managing ADE's internal and external networks. However, some IT functions, including some system development efforts, occur within other ADE units, such as the School Finance unit.

As of June 2006, ADE's IT section reports that it had 57 FTEs with 7 vacancies in 9 functional groups, as follows:

- Development (23 positions, 5 vacancies)—This group is responsible for the IT systems' analysis, design, testing, implementation, and maintenance.

- Requirements, Analysis, and Testing (7 positions, 0 vacancies)—This group is responsible for analyzing business needs, translating those needs into IT requirements, developing testing scenarios, and conducting software testing.

- Program Management (6 positions, 2 vacancies)—This group is responsible for feasibility studies related to software solutions, coordinating estimation teams, developing project plans, providing customer liaisons, assisting in prioritizing projects and maintenance efforts, and managing projects.

- Network Services (4 positions, 0 vacancies)—This group is responsible for administering and maintaining ADE's computer network and communications services.

- Database Administration (2 positions, 0 vacancies)—This group is responsible for the design and creation of new databases, the maintenance and security of existing databases, the monitoring of ADE's file storage capacity, and the backup and recovery of data maintained on ADE's network.

- Desktop Support (4 positions, 0 vacancies)—This group provides computer hardware and software support for ADE's five locations in Phoenix, Flagstaff, and Tucson; user training; equipment and software inventory control; and audio-visual support; and develops IT purchasing standards and ensures compliance with those standards when IT is purchased.

- Phone Support (3 positions, 0 vacancies)—This group provides technical support for both internal and external users of Web-based IT systems, and for internal users on agency-wide applications.

- Web Site Maintenance (1 position, 0 vacancies)—This individual is responsible for maintaining the content of ADE's Web site for all agency units, tracking and reporting on Web site usage, and assisting with Web-based presentations.

- Administration (7 positions, 0 vacancies)—This group consists of the chief information officer, an administrative assistant, and the directors of the units above.

In fiscal year 2006, according to ADE's Business and Finance unit, the total IT section budget was approximately $5.7 million. The IT section's budget is partially funded by other divisions within ADE through a cost-recovery model.[1] The IT section's $5.7 million budget also consists of Proposition 301 monies for SAIS maintenance, and federal funds for program development related to federal requirements. In addition to the IT section, some divisions within ADE also have small IT staffs and expend monies on IT-related activities that are separate and apart from the IT section's expenditures.

Scope and methodology

This audit focused on information management within ADE and covered five areas: security over ADE's IT systems and resources, SAIS data reliability, IT project management and operations oversight, the IT section's ability to meet ADE's business requirements, and ADE's compliance with student-level data collection

[1] In fiscal year 2006, this included approximately $500,000 in current-year funding and $200,000 in carryover from previous fiscal years.

notification and disposal requirements. This report presents five findings and associated recommendations, as follows:

- **ADE needs to improve its management of information technology (IT) security.** Although auditors found no evidence that sensitive information has been exposed, auditors found a lack of adequate security over ADE's Web-based applications. ADE needs to address important security concerns and should consider creating a position with specific responsibility for IT security;

- **ADE can take additional steps to improve SAIS data accuracy and functionality.** Although ADE has some data validation controls, enhancing those controls would help further ensure data accuracy. In addition, providing the ability to archive SAIS reports would allow users access to historical data. ADE could also take steps to help improve SMS software packages by monitoring performance and should consider rating or certifying these packages;

- **ADE needs to improve management of the IT systems it develops and of its IT operations overall.** A more structured process for developing and maintaining its IT systems would help ensure that systems are developed appropriately and that they can be maintained effectively. Performing activities such as regularly monitoring key performance measures, conducting risk assessments, and maintaining and testing a business continuity plan would help ADE ensure effective IT operations;

- **ADE needs to better coordinate its IT efforts in order to ensure that IT is capable of meeting ADE's business requirements, and that it properly aligns with ADE's goals and priorities.** ADE's IT section lacks an effective strategic planning process, and steps should be taken to ensure that it adequately plans. ADE should consider the placement of IT within the organization to ensure that IT requirements are appropriately addressed; and

- **ADE has not fully complied with statutory requirements for student-level data collection notification or information disposal guidelines.** ADE should comply with reporting requirements by adding, to its Web site listing of SAIS data elements, a reference to the statutory authority necessitating the collection of each SAIS data element. ADE should also develop guidelines for removing outdated data from SAIS.

Several methods were used to study the issues addressed in this audit. Methods used in all areas included interviews with ADE management and staff and other stakeholders, including district, school, and charter school staff. Auditors also reviewed Arizona Revised Statutes, and several ADE documents such as policies and procedures, strategic plans, and budget documents. A number of best practice

guides were also reviewed.[1] In addition, the following methods were used in reviewing each specific area:

- To evaluate the security of ADE Web-based applications, auditors and an independent security consultant retained by the Office of the Auditor General tested the Web-based applications using both automated and manual security testing techniques. To determine the status and effectiveness of ADE IT security controls, auditors reviewed ADE IT security-related policies and procedures and interviewed ADE staff. Auditors also performed manual testing of ADE IT security procedures to determine effectiveness. To determine actions taken to correct known security weaknesses, auditors reviewed past security assessment reports, interviewed appropriate ADE staff, and performed work to determine whether corrective actions were taken. Auditors also reviewed IT security standards published by GITA, industry best practices, and federal IT security guidelines.

- To evaluate the reliability and processing performance of SAIS, auditors interviewed representatives from GITA, the Arizona School Administrators, and several vendors of Student Management System (SMS) software products. Additionally, auditors obtained and reviewed ADE documentation on SAIS, including system documents, user manuals, and problem tickets, and reviewed professional literature. To determine how other states maintain data reliability and processing performance in their data management systems, auditors interviewed other states' education agencies.[2] Auditors also conducted a statewide, Web-based survey of individuals who enter or review student data that is submitted to SAIS. The purpose of the survey was to gather information about the process of working with and correcting SAIS data errors; the quality of ADE documentation, training, and support; and satisfaction with SMS vendors. The survey was conducted between January 12, 2006 and January 30, 2006, and was e-mailed to business officials who work for school districts, charter schools, and charter holders. A total of 774 individuals received the e-mails. However, auditors requested that e-mail recipients forward the survey on to any staff in their district or charter who enter or review SAIS data. In total, auditors received

1 Best practice materials reviewed included: (1) Gallegos, Frederick, Sandra Senft, Daniel P. Manson, and Carol Gonzales. *Information Technology Control and Audit*, *2nd Edition*. Boca Raton, FL: CRC Press LLC, 2004; (2) Grance, Tim, Joan Hash, and Marc Stevens. *Security Considerations in the Information System Development Life Cycle. U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology.Special Publication. 800-64, Rev. 1*. Gaithersburg, MD: NIST, June 2004; (3) IT Governance Institute. *COBIT 4.0*: *Control Objectives, Management Guidelines, Maturity Models*. Rolling Meadows, IL: IT Governance Institute, 2005; (4) Ross, Ron, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rodgers, and Annabelle Lee. *Recommended Security Controls for Federal Information Systems. U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology. Special Publication 800-53*. Gaithersburg, MD: NIST, Feb. 2005; (5) Office of Strategic Planning and Budgeting. *Strategic Planning and Performance Measurement Handbook, 3rd revision*. Phoenix: OSPB, Jan. 1988.

2 Auditors interviewed staff at the California, Delaware, Florida, Massachusetts, Michigan, Ohio, Texas, and Wyoming Departments of Education. These states were selected because they represented educational systems similar to Arizona's, had an IT system in use for more than 1 year, assigned unique IDs to students, were using or moving toward use of data warehouse for storage, provided other agencies with the ability to look up student information, and were recommended by other interviewees.

338 responses. The majority of the survey responses came from those required by statute to submit student data to SAIS. Specifically, 158 (47 percent) of all survey responses were from district offices, and 95 (28 percent) were from charter schools. In addition, auditors received survey responses from 52 (15 percent) district schools, 31 (9 percent) charter holders, and 2 (1 percent) third-party groups (a technology consortium and an independent company) who provide SAIS technical support to charter schools and districts.

- To determine if ADE provides adequate management and oversight of its information technology systems development processes and its IT operations, auditors observed IT systems and processes; reviewed ADE's project methodologies, procedures and policies, and system documentation; and reviewed and applied information technology management best practice information.

- To determine if ADE has established processes to ensure that IT is aligned with its business needs and whether the IT section has developed a sufficient strategic planning process to provide guidance and direction to its efforts, auditors reviewed ADE planning and budget documents, and reviewed and applied information technology management best practice information.

- To determine whether ADE is in compliance with student-level data collection notification and disposal requirements, auditors reviewed applicable statutes and consulted with legal counsel.

- To develop the Introduction and Background section, auditors compiled information from state laws, interviews with agency officials and staff, unaudited information from ADE's Web site, federal government Web sites, and agency-prepared documents such as organization charts, budget, and staffing information.

Due to the technical nature of certain terms used in this report, a glossary of IT-related terms is presented.

This audit was performed in accordance with government auditing standards.

The Auditor General and staff express appreciation to the Superintendent of Public Instruction and the Arizona Department of Education and its staff for their cooperation and assistance throughout the audit.

FINDING 1

ADE needs to better manage security of its information technology systems and operations

ADE needs to improve its management of information technology (IT) security. Lack of adequate security over its Web-based applications has resulted in exposure of sensitive information and has left these applications susceptible to many critical and well-known vulnerabilities. In addition, important IT security policies and procedures are either missing or are ineffective, and ADE has not taken sufficient action to address previously known IT security problems. To ensure that ADE adequately protects its information and technology resources, it needs to take a number of actions and should consider creating a position with specific responsibility for IT security.

Sensitive information exposed and system vulnerabilities exist

Sensitive information has been exposed due to security weaknesses in ADE Web-based applications, which contain critical flaws, also referred to as vulnerabilities, that could put them at further risk. Although auditors found no indication that these security weaknesses have been exploited or that sensitive information has actually been compromised, the mere existence of these weaknesses makes either possible.

ADE makes extensive use of Web-based applications accessible both over the public Internet and through its internal network for use by its own staff. These applications are used primarily to collect and report on information relating to students, teachers, and schools in Arizona. A review of security over several of the most frequently used applications revealed that some sensitive information could be viewed by individuals who have no right or need to access it. In addition, the review found that ADE applications were susceptible to a number of critical and well-known vulnerabilities, which could potentially lead to further compromise of systems and

information maintained by ADE. In response to these findings, ADE has taken some steps to address weaknesses in its Web-based applications.

ADE uses Web-based applications to collect and report information about students, teachers, and schools.

ADE Web-based applications used extensively—ADE has approximately 76 active Web-based applications, such as those related to teacher certification, child nutrition, grants management, and SAIS. These applications are used for a variety of purposes, such as to collect and report on information about students, teachers, and schools in Arizona. For example, student data, such as student names, birthdates, and information about when students attend or are absent from school, is submitted by school districts and charter schools through Web-based applications. Information on certified teachers in the State, such as teachers' names, birthdates, and social security numbers, is also collected and is accessible through these applications. Most of ADE's Web-based applications are available over the Internet to external users, such as school district, school, and charter school officials, and to internal users such as employees at ADE. ADE reports that approximately 3,300 different organizations and more than 13,600 individual user accounts have access to at least one of these applications.

Sensitive information exposed—A review of security over several of the most often-used applications revealed that information, including some of a very sensitive nature, was exposed and could be viewed by individuals who have no right or need to access it. However, auditors found no indication that such information maintained by ADE has been compromised.

The Office of the Auditor General contracted with an independent consulting firm to assist with an assessment of 12 Web-based applications maintained by ADE. The Web-based applications examined included those that are the most frequently used and that contain and process the most sensitive information. For example, applications that allow users to search for teacher certification information, and to submit and view student data, were reviewed. The results of this review revealed multiple circumstances that would allow a hacker or other unauthorized individuals to obtain access to personally identifiable information, including social security numbers. The review also found that hackers or others could obtain access to technical information about the applications, potentially providing hackers with additional avenues of attack.

An independent review found that a hacker could access social security numbers.

Web applications contain critical vulnerabilities—Sensitive information is exposed because all 12 of the Web-based applications auditors reviewed contained a number of critical vulnerabilities. These flaws could potentially result in ADE's systems and the information contained within them being further compromised.

Auditors identified 8 different types of critical vulnerabilities—including 4 classified as high risk—in the 12 applications reviewed. Most of the applications contained at least five vulnerabilities. These weaknesses could potentially:

- Enable an attacker to obtain access to other users' accounts or perform functions for which they are not authorized;
- Enable an attacker to view sensitive files or information; or
- Provide attackers with useful information that could assist them in carrying out further attacks.

The eight types of vulnerabilities that auditors found at ADE are considered critical and are well-known in the Web application development and security fields.

All eight types of vulnerabilities are critical and well-known in the security field.

ADE has taken some actions to address weaknesses found in its Web-based applications—In response to the Web-based application vulnerabilities found in this audit, ADE began to take steps to identify critical applications and prioritize actions needed to assess and correct discovered vulnerabilities. These actions included developing a plan to focus the efforts of its systems development staff over a 60-day period on discovering and correcting vulnerabilities it has identified in its critical Web-based applications. ADE management asserts those activities were performed during May and June 2006. ADE also developed security reference guides for developers to use when creating and maintaining Web-based applications.

ADE has not adequately addressed important security concerns

In addition to the security problems found with its Web-based applications, auditors also found that ADE has not adequately addressed a number of important security concerns. For instance, significant IT security policies and procedures are either missing or are ineffective. Additionally, ADE has not taken sufficient action to address known security problems raised in previous security assessments or identified by ADE itself.

Significant security policies and procedures are missing or ineffective—Establishing an effective set of policies and procedures to address IT security is critical to ensuring that computer systems and the information contained within them are properly controlled and used. However, auditors' review of 13 significant IT security objectives found that ADE is either missing or has ineffective polices and procedures over most of these areas.

IT best practices guidelines and policy established by Arizona's Government Information Technology Agency (GITA) highlight the importance of and need to establish and communicate policies and procedures over IT processes, including security. For example, a GITA standard addresses the need to establish rules for appropriate use and protection of data, including classifying data as either public

or confidential. This helps to ensure that agencies direct the appropriate amount of resources to protect sensitive and critical information.

ADE does not have effective security policies and procedures.

However, auditors' review of ADE's efforts to address a number of important security objectives revealed that ADE has not established effective policies or procedures. As shown in Table 1 (see page 13), while ADE had established an adequate policy for some of the areas reviewed, most areas were missing well-defined, complete, and appropriately implemented procedures that specified how it would achieve those objectives. In addition, in most cases auditors found that although ADE had procedures in place, they were ineffective in achieving the desired objective. For example, while ADE has a policy that calls for monitoring user access by maintaining access logs, it has not developed well-defined procedures or appropriately implemented the policy. While ADE keeps access logs, it reports that it does not routinely review the logs to identify unauthorized or abnormal events. Further, in the account management area, auditors found that ADE does not have a policy to address important issues such as regularly monitoring all user accounts and closing them when they become inactive. While ADE follows some account management procedures, they are not complete or appropriately implemented. In addition, the procedures they do have contain weaknesses that could allow someone to obtain an unauthorized account or to have privileges inappropriate to their duties.

In order to address these deficiencies, ADE needs to identify specific security objectives that are appropriate for its systems and users, assess its current set of policies and procedures against those objectives, analyze any gaps that are identified, and after considering the risk associated with each, develop a plan to implement effective policies and procedures. ADE then needs to monitor them on a regular basis.

ADE has not taken sufficient action to address known security problems—Although ADE has been made aware of many security concerns through previous security assessments, it has not always taken sufficient action to address them. Additionally, it has not developed a coordinated or consistent approach to ensure that it does address security concerns that it identifies or that come to its attention.

ADE has had two external security assessments in recent years, but has often failed to take sufficient action to address problems found. According to ADE, in response to an attack in which a hacker defaced ADE's Web site in 2002, ADE contracted for a vulnerability assessment to provide a comprehensive set of security recommendations. ADE indicated that in 2004, one of its major software vendors provided an even more comprehensive security assessment of its systems at no cost. Several different reports were produced as a result of the 2004 review. While ADE indicated that it has addressed the specific vulnerabilities found in the 2002 review, it has not fully considered or addressed several important findings from the 2004 assessment. For example, the 2004 assessment

ADE has not addressed several serious security weaknesses identified in 2004.

Table 1: Analysis of IT Security Objectives at ADE

Security Objective[1]	Policy Adequate	Procedure Effective	Objective Achieved
Configuration Management—Establish a configuration management program to provide accountability for changes to devices and/or associated software components.	✓		
Data Classification—Classify electronic data according to its degree of sensitivity in order to establish and apply proper security measures to adequately protect the information.			
Account Management (Web-based application accounts)—Manage information system accounts to ensure access is limited to authorized users.			
Control Deficiencies Identification—Assess security controls in the information system to ensure the appropriate security level is maintained.	✓		
Deficiencies Correction—Develop and update a plan of remedial actions to correct any known deficiencies.			
Security Update (Patch) Management—Identify, monitor, and update information systems to ensure that appropriate security updates are applied to affected IT systems.			
Password Security (Web-based application accounts)—Establish, implement, document, and communicate rules governing passwords to ensure that critical systems are safeguarded from unauthorized access.	✓		
Network Vulnerability Assessment—Scan information systems and networks routinely to identify potential weaknesses, measure risk, and eliminate vulnerabilities.			
Basic Security Awareness—Expose all computer system users to basic information about IT system security issues to ensure that IT security responsibilities are understood and followed.	✓		
User Access Monitoring—Supervise and review computer system user activities to detect unauthorized access or abnormal activity.	✓		
Intrusion Detection—Monitor events on the information system and network in order to detect attacks, identify unauthorized use of the system, and take appropriate remedial action.			
Media Cleansing—Ensure that data is irretrievably removed from information system digital media, such as hard drives, when such media is no longer needed.	✓		✓
Mobile Device Security—Establish guidelines and requirements for portable and mobile devices to ensure protection of IT resources and sensitive information.			

1 Security objectives were developed based on standards promulgated by GITA, guidelines established by the National Institute of Standards and Technology, and the Control Objectives for Information and Related Technologies established by the Information Systems Audit and Control Association.

Source: Auditor General staff analysis of selected ADE IT security policies and procedures, as of April 6, 2006.

highlighted some common but potentially serious weaknesses in some of ADE's Web-based applications, network security, and internal processes. While ADE did fix some specific weaknesses found in its Web-based applications, it has indicated that other weaknesses noted in the reports were not addressed. Several of these weaknesses were critical and should have been addressed immediately. ADE personnel indicated that many security weaknesses have not been addressed because they lack needed resources, because of the difficulty in scheduling system downtime needed to address weaknesses, and because of an agency-wide lack of focus on security.

Further, ADE has indicated that it did not use the results of its 2004 review to assess whether its other Web-based applications had similar problems to those found, nor did it take action to ensure that it prevents future problems by including more focus on security as it develops new applications. For example, ADE has not fully established guidelines to identify and address security requirements during its software development and testing processes. In addition, staff responsible for developing and testing ADE's computer applications did not feel they had been properly trained to recognize and address security vulnerabilities.

ADE has also identified a number of security concerns on its own and has reported these on its 2005 and 2006 Technology Infrastructure Standards Assessment (TISA) report, which is submitted to GITA on an annual basis.[1] However, it has only recently begun to take action to address some important items. For example, ADE's 2006 TISA indicates that it does not test its backup data for restorability or classify its data according to risk. However, ADE has only recently developed a preliminary plan for testing backups and does not currently have any specific plans in place to address data classification. ADE indicates that for many of the weaknesses noted in the TISA reports, corrective action is either in progress or it lacks adequate resources to implement a corrective action plan.

ADE does not have plans in place to classify data according to risk.

Finally, ADE has indicated that it has not had a coordinated approach for addressing security concerns that it identifies or that come to its attention. Security issues that have been addressed or corrected in the past were done by individual initiative rather than in a coordinated and consistent way. ADE should develop a specific process to evaluate its known security concerns, prioritize them in order of risk, develop a plan to address them, and ensure that responsibility for correcting them is appropriately assigned. ADE should also develop a process to identify and implement specific security guidelines for its systems, incorporate them within its systems development and testing process, and train its development and testing staff on security concerns and methods.

[1] The TISA is a self-assessment required by GITA to help agencies identify their IT security vulnerabilities. In 2005, it was called the Technology Security Assessment.

ADE should consider assigning responsibility for IT security

ADE should consider creating an appropriate position to be responsible for all IT security within ADE. If established, this position should be charged with responsibility for achieving the actions recommended in this report and for routinely conducting an agency-wide assessment of IT security policies and practices to ensure that agency security objectives are met. This would help to further raise security awareness within ADE, establish security as an ADE priority, and ensure that someone is accountable for addressing security-related issues and concerns.

Leading organizations establish centralized security responsibilities.

The U.S. Government Accountability Office (GAO) found that leading organizations establish centralized security responsibilities over information security practices.[1] GAO indicated that this enabled those organizations to achieve some efficiencies and increase consistency in the implementation of their security programs. Further, best practices indicate that when assigning such responsibility, it should be:

- Established at the organization-wide level to enable effective actions with organization-wide security issues and should be independent of day-to-day IT operations; and

- Embedded at an appropriate senior level to enable effective design, implementation, and enforcement of the organization's security policies and procedures.

1 U.S. Government Accountability Office. *Executive Guide: Information Security Management (GAO/AIMD-98-68)*. Washington, D.C.: GAO, May 1998.

Recommendations:

1. ADE should develop and implement an ongoing process for addressing IT security vulnerabilities or control weaknesses when they are discovered. The process should ensure that known security concerns are evaluated and prioritized in order of risk, that specific plans to address them are developed, and that responsibility for correcting them is assigned.

2. ADE should identify specific security objectives, assess its current set of policies and procedures against those objectives, analyze any gaps, consider the risk associated with each, develop a plan to implement effective policies and procedures, and monitor them on a regular basis.

3. ADE should develop a process to identify and implement specific security guidelines for its systems, incorporate them within its systems development and testing process, and train its development and testing staff on security concerns and methods.

4. ADE should consider creating an appropriate position to be responsible for all IT security within ADE. The reporting line of the security position should be such that it can effectively design, implement, and enforce compliance with the organization's security policies, standards, and procedures, and ensure that they are functioning effectively.

FINDING 2

ADE can further enhance SAIS' reliability

ADE can further improve SAIS' reliability and processing performance. SAIS processes and maintains a large amount of valuable data, and its success requires the cooperation of all parties involved, including school districts and charter schools who record and submit the data, vendors who develop the majority of the software packages used to submit data, and ADE. According to a survey conducted by our Office, although the majority of SAIS users have confidence in the accuracy of SAIS' data, some users continue to raise concerns. As the primary entity responsible for maintaining and operating SAIS, ADE plays an important role and can help further improve SAIS reliability by doing three things: (1) adding more controls to ensure data accuracy, (2) taking basic steps to improve functionality, such as providing the capability to archive reports, and (3) monitoring the performance of the various SMS software packages and possibly establishing a rating or certification process.[1]

SAIS processes and maintains a large amount of valuable data

SAIS collects and processes student data that is used for determining academic progress, meeting state and federal reporting requirements, and most importantly, according to ADE representatives, data within SAIS is the basis for calculating ADM and distributing approximately $3 billion in state funding for education. SAIS continuously evolves because SAIS data requirements may change from year to year because of state education mandates. In addition to data processing within SAIS at ADE, the operation of SAIS involves significant data processing at the district, school, or charter school level. A.R.S. §15-1042(B) requires school districts and charter schools to submit student-level data to SAIS. There are approximately 700 districts and charter schools.

These entities use SMS software packages to record and process information locally and transmit the required student-level information to SAIS.[1] Once data is received

1 Districts, schools, and charter schools use SMS software packages to store and manage student information and submit electronic information to SAIS.

SAIS Processing Data
(Unaudited)

Fiscal Year 2005

- 43.4 million—Approximate number of total student data transactions.
- 39.5 million—Approximate number of transactions successfully processed.
- 3.9 million—Approximate number of transactions that failed processing.
- 96,600—Approximate number of transaction failures due to system errors (i.e., caused by software operating system, hardware failures, etc.)
- 91 percent—Overall success rate of all transactions processed.

Fiscal Year 2006

- 46.5 million—Approximate number of total student data transactions.
- 42.4 million—Approximate number of transactions successfully processed.
- 4.0 million—Approximate number of transactions that failed processing.
- 145,000—Approximate number of transaction failures due to system errors.
- 91 percent—Overall success rate of all transactions processed.

Source: Auditor General staff analysis of transaction information provided by the Arizona Department of Education from SAIS for fiscal years 2005 and 2006.

at ADE, to help ensure data accuracy, SAIS conducts three different levels of data validation, with the first applied to the file submitted and the next two applied to records, or transactions, within the file. In fiscal year 2006, districts and schools submitted more than 46.5 million transactions, and according to an ADE report, approximately 9 percent of the transactions submitted failed. Failures can result from a number of factors, including data entry errors by school districts and charter schools, SMS software issues, or ADE issues such as system failures. As such, the success of SAIS requires the cooperation of all parties involved, including those who record and submit data, ADE, and the vendors who provide a majority of the SMS software packages used.

Concerns regarding SAIS

Some SAIS stakeholders have raised concerns about SAIS data reliability and the additional resources required to work with SAIS both recently and in the past. For example:

- **Data accuracy concerns**—Although the majority of SAIS users surveyed for this audit have confidence in the accuracy of SAIS data, some concerns continue to be voiced. In 2004 and again in 2005, the Arizona School Administrators adopted a formal position that "the data within the system is unreliable. The lack of reliability has a direct impact on both funding and academic performance."

1 In addition to districts and charter schools submitting data to SAIS, auditors learned that district schools may also submit student-level data to SAIS using SMS packages. According to agency information, there are approximately 1,600 district schools in Arizona.

Similarly, 29 percent of the SAIS users surveyed for this audit reported that they were not confident that the data in SAIS was accurate when it was needed for final reporting or funding purposes. In addition, more than one-third of survey respondents reported that they had experienced problems with student data being dropped or disappearing from SAIS.

- **Resource concerns**—Some SAIS users expressed concerns about the time and money required to work with SAIS. One survey respondent reported, "SAIS has cost our district a lot of time and money. Time-consuming administrative requirements and burdens are continually added . . . We had to add staff to handle SAIS duties with no additional dollars." Another survey respondent stated that because of the complexity of SAIS and their SMS package, the district felt the need to attain outside assistance, which cost more than $25,000. According to the respondent, this was a "massive amount of money" for the district. Similarly, one third-party respondent who assists several schools and districts in working with SAIS stated, "An overriding concern of administrators is the huge amount of staff time required for SAIS reporting . . . In a time when there is a continual push to lower administrative costs, this is a tremendous burden."

  Concerns about the resources required to work with SAIS are not new. In 2003, the Pima County School Board/Superintendent Collaborative sent ADE a letter expressing similar as well as other concerns. Auditors spoke with a collaborative representative who indicated that ADE worked hard to address many of the issues and did so successfully. However, the representative also indicated that SAIS is not a user-friendly system, requiring major staff efforts to ensure accuracy, and that at this point, most have just accepted that reality.

ADE should take additional steps to improve SAIS data reliability and processing

ADE can further improve SAIS. Although some controls exist, ADE needs to implement additional controls to better ensure that data submitted by users and processed through SAIS is accurate, complete, and current. In addition, ADE can take steps to improve SAIS' functionality by making modifications, such as providing the capability to archive reports.

SAIS controls could be enhanced—As indicated on page 18, ADE has established some data validation controls, and enhancing those controls would help further ensure data accuracy. Controls are used in computer applications to ensure complete processing and data integrity. Auditors reviewed two main types of controls—input and process. Input controls help ensure the accuracy of data as it is entered into the system, while process controls help ensure that no data is lost inside the system. Both can be improved as follows:

- **Input controls should be improved**—SAIS has some types of input controls in place, but entirely lacks one type of input control. The first type of input controls, file checking, ensures files received from users can be processed by SAIS. For example, if SAIS cannot accept the file because the file size is too large or the file's general structure is incorrect, the file is sent back to the user to be corrected. The second type of input control, data validation, ensures a basic level of data accuracy and completeness; for example, a gender field being checked to contain only the values "M" or "F," or a birthdate field being required.

  ADE lacks a comprehensive, department-wide documented process for developing and implementing the business rules that support a third type of input control, integrity checking. Integrity checking verifies that the data submitted complies with business rules. According to ADE, business rules are derived from statutory requirements and ADE policy, such as requirements related to public education reporting or funding. Although some units, such as the School Finance unit and the IT section, have drafted some procedures for establishing business rules, these procedures have not been formalized. Instituting a comprehensive, department-wide process for implementing business rules is important since new rules are added on a regular basis, and such a process could help ensure all appropriate business rules are effectively established. Auditors were told of some instances where business rules were established, but did not work as intended. However, auditors were unable to pinpoint why this happened because ADE's process has not been formalized and lacks adequate supporting documentation. For example, ADE was unable to successfully implement a business rule stating that a student must not have graduated from the highest grade taught in the school district to be eligible for state aid. This requirement should apply only to high school graduates. However, the business rule was incorporated into SAIS in such a way that it was preventing some other students from receiving funding, such as those graduating from 8th grade. As a result, ADE needed to disable the rule, but is working to revise and implement it for fiscal year 2007.

  Integrity checking verifies that data submitted complies with statutory requirements.

  To help ensure appropriate business rules are completely and successfully implemented, ADE should should establish a department-wide, comprehensive procedure. This procedure should include all the steps from identifying what rules are needed to implementing those rules in SAIS. This procedure should also ensure that all appropriate parties are involved in every stage of the process, such as the conceptualization of the rules, requirements development, and the review and approval of testing results prior to implementing the rule in SAIS. ADE may find that this procedure could be developed through its Student Detail stakeholders meetings facilitated by the System Training and Response (STaR) team. This group is working to coordinate the interests of all ADE unit staff who work with SAIS and IT staff are regularly invited participants.

  ADE lacks controls to verify that all data complies with all statutory requirements.

  A fourth type of input control, automated variance checks, does not exist in SAIS and should be implemented. Variance checks call attention to unusual

differences in data, such as a large change in the number of students from the prior year. According to ADE's School Finance unit, the unit currently conducts manual variance checks for some charter schools by comparing current charter school data to previous data used for determining funding. School Finance unit staff report that the manual variance checks are not done to identify errors made by the schools in submitting the data, but rather to ensure that no SAIS problems have caused the errors. The unit does not review every charter school's data, but rather unit staff look for those schools that may experience drastic funding cuts. According to the unit, the threshold established to select the charter school data in need of further investigation is set at a high level. However, the unit reports working within the resources and time available to conduct the variance checks.

SAIS lacks variance checks that call attention to unusual differences in data.

ADE could improve this manual process by establishing automated variance checks that would look at the data for all districts and charter schools rather than just certain charter schools. To determine what types of automated variance checks would be the most valuable, ADE should ensure that appropriate staff, such as IT staff and other ADE business units using SAIS data, are involved in identifying, developing, testing, and implementing these checks. An important part of implementing automated variance checks would also include assigning responsibility for following up on any data variances that appear unreasonable, and determining at what point or points in the process to include these automated variance checks.

- Automated process controls should be implemented—Although some manual process controls exist, SAIS does not have any automated process controls. Best practices state that process controls are used to ensure that no data is added, lost, or altered during processing. Many survey respondents complained of data being "dropped" or "disappearing" from SAIS. Although the data may still be somewhere in the system, it is not moving forward and counted by ADE's School Finance unit for school funding. This often results in ADE's School Finance unit having to reconcile the data manually, or requires manual intervention from IT staff to resolve. In addition, without process controls in place, users may or may not find the causes of inaccuracies with their data.

SAIS lacks automated process controls that ensure that no data is added, lost, or altered during processing.

ADE should add some process controls such as run-to-run totals and data reconciliation. These types of checks, run at key points in the process, would help ensure that when individual student-level data is uploaded or moved from one SAIS process to the next, that no data is lost or altered. If the process controls alert the user to potentially lost data, the problems can be found, and the failed processes can be corrected. Once implemented, process controls should be run and reviewed at least twice a month in an attempt to prevent potential problems with SAIS data

SAIS functionality can be improved—ADE can take some basic steps to improve SAIS' functionality with minimal impact to resources. ADE is in the process of implementing one change. In addition, establishing a tactical team would help ADE determine and prioritize other stakeholder needs.

- **ADE should continue to develop and provide archived, funding-related reports to SAIS users**—Providing archived reports in SAIS would improve users' ability to reconcile student data and ensure that ADE calculates correct funding. Currently, with one exception, SAIS has the ability to retain only the most current version of reports, meaning if there is a processing problem, users cannot obtain previous reports from SAIS to correct the situation. Having archived reports would alleviate this problem. Auditors interviewed a SAIS user, who described a situation where reports they saved allowed a charter school to retain funding for students who had legitimately attended the school. Had the issue not been resolved, ADE would have taken back all of the money previously given to the school for the students whose records were in question. Schools also need to compare data processed each month with data processed from previous months to ensure student data has been processed by SAIS. Their ability to make such comparisons would be enhanced if SAIS included a place where past records could be archived for retrieval at any time.

  In fiscal year 2006, the IT section developed a tool for archiving one funding-related SAIS report, but user acceptance is still needed. This report displays the results of the most recent aggregation for average daily membership and average daily attendance by grade level, school, and reporting period. Other than this report, SAIS has the capability to retain only the most recent version of reports. SAIS users can pull data reports that provide various types of information about the data, including unadjusted counts of students at schools, adjusted counts, and special education information. However, a user must keep printed copies of such reports in order to refer to them at a later time. Therefore, ADE should obtain user acceptance of the one report it has developed for archiving, and also work to develop and implement additional archived reports. As part of this process, ADE should ensure that appropriate SAIS stakeholders are involved in determining what funding-related SAIS reports should be archived, as well as in user acceptance testing.

Archived reports could facilitate schools' month-to-month data comparisons.

- **ADE should establish a tactical team to address its users' needs**—ADE should establish a tactical team composed of the ADE IT section and other internal and external stakeholders to determine and prioritize changes to SAIS that will help address SAIS users' concerns. The tactical team should focus on changes that are the most feasible, such as those that will have the biggest impact and can be done with a reasonable amount of resources. For example, the tactical team might consider whether producing reports mid-month, which ADE's school finance staff believe would allow the unit and charter schools to identify errors that need to be corrected for accurate payment calculations in a more timely manner, is something that the SAIS community feels should be

implemented. However, the tactical team would need to evaluate the impacts and the relative benefits of stopping SAIS processing mid-month to produce the reports relative to other needed SAIS changes the team may identify. Once SAIS changes are identified and prioritized, the tactical team should establish a schedule for implementing the agreed-upon SAIS changes.

ADE should take steps to improve oversight of Student Management System (SMS) software performance

In addition to the changes needed in SAIS, ADE should improve its oversight of the SMS software used by districts, schools, and charters to submit student data to SAIS. Auditors' survey of SAIS users and a review of data submission error reports identified problems with software performance. There are several reasons SMS software package quality varies, including ADE's failure to monitor software performance. ADE can encourage improvement of software performance by ensuring its SAIS SMS software test environment is up-to-date and available, monitoring software performance, and possibly establishing an SMS software rating or certification process.

Many software packages used with varying levels of quality—The numerous software packages developed to collect and transmit student information to SAIS vary in their ability to successfully submit data. According to agency information, at least 20 different software packages, developed either by districts or purchased from outside vendors, are used to collect and transmit student data to SAIS. However, auditors found that the quality of these products varies considerably. At auditors' request, ADE generated a report of the type and amount of transaction errors associated with each software package submitting data to SAIS during fiscal years 2005 and 2006. According to the report, during fiscal year 2006, one software package had an error in 0.7 percent of the transactions submitted to SAIS, while another software package had a 31.8 percent error rate. These errors can have various causes, including issues with SMS programming that can result in errors when the data is correct. Regardless of the causes, whenever these errors occur, districts, schools, and charters must resubmit their data, and SAIS must then reprocess it, which requires additional time on the part of the district, school, and charter staff, and additional ADE resources.

At least 20 different software packages with varying quality are used to collect and transmit student data to SAIS.

In addition, auditors found that when users upload electronic files of student data records to SAIS and are notified that a few records have an error, a few software packages require that full files be sent back through SAIS instead of only the records that have been repaired. According to ADE, this can create unnecessarily large files, when fixing only the incorrect record or records through a change transaction could have resolved the issue. For example, if a student were incorrectly marked as being in first grade, but is really in second grade, a change

transaction would correct just the student's grade. However, some SMS software packages address corrections like these by deleting the student and all associated information from SAIS, and then resubmitting the student and all other data associated with that student. According to ADE, there is always a chance that during this type of error correction process, something could be coded incorrectly and the student's data would never get added back into SAIS.

Some software packages may vary in quality because ADE has not established clear guidelines. For example, although ADE provides vendors with information about internal SAIS controls that check the basic accuracy and completeness of submitted data, the agency does not require vendors to include these controls in their software. ADE hopes that vendors will include these controls to reduce ahead of time the amount of errors identified in data submitted to SAIS. As a result, the five vendors that auditors interviewed varied in the amount of controls they include in their software. For example, two vendors stated that they implement all the error checks they can while another stated that they offer only some error checks.

Users concerned with SMS software performance—Auditors' survey of SAIS users identified concerns with software performance. For example, one district who was using a particular vendor reported that they lost all of their kindergarten data during the SMS software package's automatic process of updating student records to reflect the students' change to first grade. The district had to create a new file for the prior year so they could receive their ADM for those kindergartners. This district has since switched to another SMS software program and feels the software has allowed them "a better start." Another district reported, "We have had software issues that have taken a long time to address, and I question why the software was not tested more thoroughly before release to schools." Finally, a charter school respondent provided the following feedback: "We believe that many of our problems with SAIS data originated with the interface between (the vendor product) and SAIS." Although some survey respondents voiced frustration about the vendors' role in software performance, survey respondents clearly felt that some of the responsibility fell to ADE because SAIS is an ADE system.

One survey respondent said that many of their SAIS data problems originated with the vendor product and SAIS interface.

Several reasons software quality varies—Software performance varies for several reasons, as follows:

- ADE has relaxed software testing requirements—ADE applied more stringent testing requirements to vendors who wished to be listed on an ADE Web list of vendors supporting SAIS when SAIS was first established. The initial tests required vendors to successfully submit to SAIS a variety of student data file transactions, such as files related to student absences, student assessment information, and Special Education program participation. Vendors were also asked to demonstrate that their software could successfully submit data representing a variety of cases, such as a student registering for the first time at a school, but who also failed to attend. According to ADE, each vendor was

also assigned to work with an ADE employee throughout the process. If a vendor's SMS software package was successful in completing all transactions and case studies, vendors and their products were listed on ADE's Web site as a "vendor supporting SAIS."

Since the initial round of software testing, however, ADE has relaxed its requirements. According to ADE, resource limitations have prevented it from continuing the original process. However, it still requires that vendors demonstrate that their software product is able to successfully submit the required student data file transactions. In addition, the vendor must provide a letter or e-mail from a client indicating that they are using the product and are satisfied with it. However, ADE no longer requires that new software products successfully complete the case studies, and it does not assign a specific ADE employee to work with the district and/or vendor throughout the process. According to ADE, only two software products have been added to the list of vendors after SAIS was implemented. However, because ADE does not require vendors to annually demonstrate that their product will work with the most current version of SAIS, one of the newer vendors was listed by ADE on its Web site even though it had only shown that its product worked with the previous year's version. This occurred even though the current version of SAIS had incorporated a number of changes.

- ADE's test environment is not always current—The test environment ADE developed for vendors and districts to test their SMS software products on is not always ready when needed. As a result, the vendors and districts developing their own SMS software sometimes do not have sufficient time to correct any software problems they may find before the software needs to be used to actually submit data to SAIS. For example, for the 2005-2006 school year, ADE's test environment was not available until after the school year began. As a result, one vendor reported having some of its clients use its untested software to submit their actual data to SAIS so that it could identify whether errors occurred and then correct the problems before providing an updated version of the software to its other clients. Finally, another vendor reported having to correct problems with its SMS software that would have been caught before its clients began using it if the test environment had been available.

  Districts and vendors do not always have sufficient time to test and correct problems before their SMS software needs to be used.

  According to ADE, the test environment was not available this year because SAIS system changes were not ready and there was not a server available for SMS software testing. ADE also indicated that keeping SAIS up and running takes priority over maintaining the test environment. Specifically, SAIS changes are implemented in SAIS and the SMS software test environment at the same time, and ADE runs tests to make sure that the changes were successful in SAIS. However, when new changes result in problems in SAIS as well as the SMS software test environment, fixing SAIS takes priority.

- **ADE does not monitor or provide assurance regarding software performance**—ADE fails to monitor SMS software packages after they are placed on the ADE list of vendors supporting SAIS and does not provide assurance that the listed software packages are successfully able to meet SAIS processing requirements. As previously mentioned, at auditors' request, ADE generated a report showing the number and type of transaction errors experienced by each software package. Auditor analysis of the report identified numerous, specific transaction types, such as those related to support program participation (i.e., submission of information related to participation in programs for block grants), and student assessments (i.e., data concerning assessments administered to a student in order to identify a language need), which experienced a failure rate of 33 percent or more by at least three different software packages. This report also indicates that most problems are associated with vendor-developed software products rather than software developed by the districts.

  Because ADE does not monitor performance, the agency does not assure SMS software performance, even though these SMS software packages may be listed on its Web site. Instead, the agency has added a caveat to the Web page listing vendors supporting SAIS stating that there was no way for the agency to verify that all transactions and files generated by the vendor's SMS software package were submitted to ADE without alteration. However, auditor analysis of the ADE-generated software package error report found that the majority of SMS software packages listed on ADE's Web page have problems submitting some transactions, regardless of when the SMS software was developed.

ADE should take actions to improve SMS software performance—ADE could take action to facilitate improvement of SMS software performance. Although ADE indicated it does not have the authority to ensure SMS software compliance, auditors found that ADE has adequate authority. Specifically, A.R.S. §§15-901(A)(15) and 15-1042(A) require ADE to prescribe the format, manner, and procedures for electronic data submission. Auditors identified three types of actions ADE should take to improve software performance, as follows:

- **Ensuring the test environment is updated**—ADE should ensure that the test environment is up to date and available for use at the beginning of the school year and at other times as needed so vendors and districts developing their own SMS software can demonstrate that their software can successfully submit the required student data file transactions to SAIS.

- **Developing a proactive means of monitoring vendor performance**—ADE should use transaction error reports, such as those generated at auditor request, to monitor and analyze software performance, identify potential problems, and perhaps provide increased assistance to vendors as a means to help identify and resolve problems with particular transactions. Monitoring and following up on identified software problems may also help ADE reduce

Monitoring and following up on identified software problems may help ADE reduce the number of files that SAIS must reprocess.

the number of files that SAIS must reprocess. ADE may also use these reports as a preliminary step to establishing software package performance standards for rating or certification.

- Rating or certifying software packages—ADE should consider rating or certifying software packages. Iowa's Department of Education certifies Student Information System (SIS) vendors whose products are used to submit data to Iowa's Department of Education. Iowa certifies vendor products twice a year and has different processes for returning and new vendors. Auditors interviewed five vendors providing SMS software packages to clients in Arizona. All five supported some type of a certification or compliance process, although some were more supportive of the concept than others. To further ensure that SMS software packages comply with SAIS requirements, ADE should work with SMS software vendors and users to determine what factors should be included in the process, how frequently the process should occur, and where to publish the results of the certification or rating process, such as on their Web site. ADE would also need to establish a mechanism for addressing vendors who do not meet the recurring certification or rating requirements. Any rating or certification process that is implemented should allow sufficient time for software developers to meet the requirements.

Recommendations:

1. To improve SAIS data reliability, ADE should implement additional controls. Specifically, ADE should:

    a. Establish a department-wide comprehensive procedure for developing and implementing business rules;

    b. Implement automated variance checks by identifying appropriate staff to determine what types of variance checks should be added, as well as assigning responsibility for following up on any data variances that appear unreasonable; and

    c. Add processing controls such as run-to-run totals and data reconciliation, and review information collected from the controls at least twice a month to help prevent potential problems with SAIS data.

2. To help improve SAIS' functionality, ADE should:

    a. Obtain user acceptance of the one report that has been developed for archiving, and

    b. Develop and implement other SAIS-archived reports.

3. To address user concerns and identify additional ways to improve SAIS, ADE should:

    a. Establish a tactical team composed of representatives from ADE's IT section and both internal and external stakeholders to identify and prioritize its user community's needs, and

    b. Establish a schedule for implementing the agreed-upon SAIS changes.

4. To improve SMS software performance, ADE should:

    a. Ensure the SAIS SMS software test environment is up-to-date and available when needed;

    b. Monitor software performance and take steps to address any problems identified; and

    c. Consider establishing a recurring SMS software certification or rating process.

FINDING 3

ADE needs to improve IT project management and operation oversight

ADE needs to improve its approach for managing systems development projects and for overseeing its IT operations. ADE's environment for developing IT projects is currently characterized by a lack of consistency, with projects being developed both inside and outside the IT section and without a clear and consistent development approach in either setting. Documentation explaining how a system functions and how to use it is often missing or of limited quality. ADE has taken some recent steps to provide direction and guidance over development activities, but additional work is needed. To ensure effective IT operations, ADE needs to (1) adopt a more structured process for developing and maintaining its IT systems and (2) improve key IT oversight activities, such as regularly monitoring key performance measures, conducting risk assessments, and maintaining and testing a business continuity plan.

IT project management approach lacking

The IT section at ADE develops IT systems ranging from relatively small applications, such as one called the Arizona State Tutor Fund, which is used to collect data for the Failing Schools Tutor Fund program, to much larger and more complex applications such as SAIS, which is used to collect state-wide, student-level data and to perform a variety of data aggregation and reporting functions that are critical to calculating state funding for education. ADE has had a recent history of ad hoc development of information systems, and that approach has resulted in several inconsistencies. These inconsistencies can be seen in where and how systems are developed, as well as in the documentation prepared to explain and support the systems.

Information systems development scattered and unstructured—Several of ADE's current information systems have been built by various development teams who in most cases have not followed a standard agency development process, resulting in information systems that are difficult to maintain

and use. IT management and staff members agree that the information systems development process within the IT section varies by team and by project. For example, according to IT developers and the Director of Requirements and Testing, the majority of changes made to SAIS go through the IT Quality Assurance Team (QA) before being put into production, but changes to other applications have traditionally not gone through a formal QA process. Instead, according to one IT developer who works on the Grants Management application, changes are usually only informally tested by users before being fully implemented. Another example comes from the Exceptional Student Services (ESS) unit that has an IT developer who works on all of the applications and databases that the ESS unit uses. The developer has built and currently maintains several important ESS information systems that are used for meeting federal reporting requirements, but does not follow a specific development process and has created minimal documentation of how the systems operate.

Some software changes are implemented without going through quality assurance testing.

Further, software applications have been developed outside of the IT section, again without a standard agency development process. According to IT management, these projects sometimes fail or develop problems that the IT section is then requested to provide assistance in correcting and/or with maintaining the information system. For example, the Certification unit is currently developing a "Teacher Certification Web System." According to the agency, this project has encountered many problems, including poor vendor relations, and at least part of the application is not usable and needs to be completely replaced.

The IT section does not oversee all software development.

ADE's IT unit management is aware of its minimal use of a systems development process and has acknowledged a need to improve. It has set a goal to correct many of the deficiencies by 2008, but does not have a documented plan for how it will reach its goals.

Key information system documentation is missing or insufficient—

Creating documentation is an important part of each phase of a good information system's development process. However, many of ADE's information systems lack good documentation, which has caused difficulties in maintaining and modifying the systems. ADE needs to take a number of steps to address these problems, such as identifying documentation gaps and adopting a plan to address them.

Documentation explains how a system functions and how to use it. Good documentation is necessary to provide easy-to-read instruction manuals for the system's users and to provide technical details that IT staff need to be able to maintain and modify the system in the future. However, since ADE has not used an adequate development process, many of the information systems that ADE created are lacking high-quality documentation. For example, a staff member who works on a system requirement's guide for part of SAIS does not have a complete data dictionary or flowchart to work with. Data dictionaries and flowcharts are important pieces of documentation that provide a description of what the data is and how it moves throughout an information system. As a result, if this staff

IT staff do not always have or maintain high-quality documentation for ADE's applications.

member leaves, the next person assigned to work with this system will likely face problems understanding how the system stores and processes data. Further, IT staff often do not keep the existing documentation updated. In the case of one application that auditors reviewed, the programmers stated that they were not sure which of the original documentation was still relevant, and when they made program changes, they did not update the design documentation.

The lack of documentation of some applications has resulted in steep learning curves for IT staff who must modify and maintain these applications. This is especially true when, due to turnover or other reasons, staff must work on applications they are not familiar with. For example, an IT staff member stated that he had to create his own documentation when he was assigned to maintain an application he had not previously worked on. The staff member described how he had to develop his own way of understanding the application; for example, he interviewed the outgoing developer, experimented with the application, and reviewed the code to become familiar with how it operates. Missing or poor documentation also leads to inefficient use of staff time. For example, the staff member mentioned above spent a day reviewing the application to understand a function that may have taken minutes to understand had he had good documentation.

Lack of an adequate development process also causes inconsistencies in the way that documentation is managed. For example, despite the challenges the staff member mentioned above faced due to the lack of documentation, he has not taken all of the steps necessary to ensure that the documentation he developed will be available to a different staff member in the future.

ADE needs to take a number of steps to address its documentation problems. First, ADE should review its current applications' technical and user documentation to determine what is needed to properly maintain its applications. Second, it needs to prioritize the gaps between existing and desired documentation. Finally, it needs to develop a plan to address the gaps and schedule improvement activities to address them.

ADE should establish effective process for developing information systems

ADE needs to institute an effective Systems Development Life Cycle (SDLC) process for developing information systems. Establishing an SDLC process will help ensure that systems are adequately developed, tested, and documented before being put into operation. Although ADE has recently taken steps to improve its development process, several additional steps are needed.

SDLC methodology helps ensure proper information systems development—An SDLC process is an accepted approach used to consider

Systems Development Life Cycle Phases and Key Deliverables

Initiation
- Needs determination:
  - —Perception of need
  - —Linkage of need to mission and performance objectives
  - —Assessment of alternatives to capital assets
  - —Preparing for investment review and budgeting

Acquisition / Development
- Functional statement of need
- Feasibility study
- Requirements analysis
- Alternatives analysis
- Cost-benefit analysis
- Software conversion study
- Cost analysis
- Risk management plan
- Acquisition planning

Implementation
- Installation
- Inspection
- Acceptance testing
- Initial user training
- Documentation

Operations / Maintenance
- Performance measurement
- Contract modifications
- Operations
- Maintenance

Disposition
- Appropriateness of disposal
- Exchange and sale
- Transfer and donation
- Contract closeout

Source: Auditor General staff analysis of NIST Special Publication 800-64 Rev. 1.

and develop an information system or to make a major modification to an information system. SDLC methodologies frequently group similar activities into phases. Typical phases are shown in the colored textbox, and each phase typically results in a number of key deliverables.

Using an SDLC process helps ensure that systems developed meet IT mission objectives, are compliant with the current and planned laws and regulations, and are easy to maintain and cost-effective to enhance. An SDLC process also provides other benefits when creating information systems, such as reducing risks and errors, helping to ensure that security requirements are integrated into applications and systems, and avoiding inefficient activities, such as recreating existing components for each project.

Additional steps needed to establish SDLC process—Although ADE has recently taken some steps to provide direction and guidance over IT development activities, additional work is needed. ADE needs to expand and further develop the project development guide that was recently published by the IT section. Further, ADE needs to ensure that all IT projects, whether developed by the IT section or other units within ADE, follow this SDLC process:

- **Expanding project development guidance**—In 2005, a Project Management Office (PMO) was created to help direct technology activities. The *Project Management & Software Development Methodology* guide, which the PMO first published in November 2005, outlines an information systems development methodology. This document provides a good start, but it needs more detail and a better plan to ensure that it is effectively implemented and that its use is monitored to ensure that it is properly followed. For example, the guide is lacking standard life cycle phases (operation, maintenance, and disposal); does not provide a plan for frequent stakeholder communication; does not integrate security into development; and does not provide detailed documentation templates. In addition, the methodology contained in the guide has not been widely promoted and is not widely used. A PMO director acknowledged that the guide needs to be updated and improved.

- **Ensuring more uniform procedures throughout ADE**—ADE also needs to ensure that all projects follow a standard SDLC. Currently, the IT section does not oversee all system development. As discussed previously, various divisions have their own IT employees who work on projects specific to their divisions, but do not have to follow the SDLC methodology the PMO promotes. According to IT management, this has not only led to problems in developing some projects, but created additional difficulties when the IT section has later had to maintain and operate the information systems. ADE should develop, adopt, and enforce the use of a single, effective, agency-wide SLDC process.

ADE should improve key oversight activities

Improving the IT oversight framework will help ADE management ensure that it can sustain operations and implement the strategies required to extend activities into the future. In particular, ADE's efforts need to address three important pieces of an IT oversight framework:

IT does not have a method for proactively identifying and addressing performance problems or vulnerabilities.

- Performance measurements—ADE needs to identify, develop, and proactively monitor key IT performance indicators. According to IT management, the IT section performs minimal monitoring of performance and of some other key indicators such as server statistics or system capacity used. ADE's IT section should develop and proactively monitor these and other performance measurements, such as the number of production problems per application that are causing visible downtime, the number of IT calls handled by the Support Center, and the number and status of requests for systems modifications. The IT section should also monitor measurements that indicate the performance of the section, such as the percentage of users satisfied with functionality of systems delivered and the availability, completeness, and accuracy of user and operational documentation.

- Risk assessments—To ensure IT risks are properly identified and mitigated, ADE's IT section should regularly perform IT risk assessments and develop procedures to address issues raised. Possible risks include such things as a hacker disrupting ADE's Web site, the loss of key personnel, or computer hardware failures. ADE has not adopted a framework to properly analyze and manage such risks. Although ADE developed a policy statement that indicates a risk assessment should be conducted twice a year, the policy is not in operation. ADE indicates that it does not have adequate resources to fully implement its policy. While some activities, like independent assessments, may require additional resources, other activities, such as a basic internal identification and ranking of problem areas, could be performed with minimal resources. Finally, ADE does not have an effective process in place to address issues that may be uncovered through risk assessments. As a result, even if risk assessments were performed and issues identified, there is no assurance that the issues would be addressed.

- Disaster recovery and business continuity planning—ADE's IT section should fully develop a business continuity plan that is updated and tested regularly. The need for providing uninterrupted IT services requires developing, maintaining, and testing IT disaster recovery and continuity plans, providing for off-site backup facilities, and establishing regular plan training and testing. ADE's IT section has produced a state-required business continuity plan, but based on auditor analysis, the plan is not adequate to address a major disruption to IT services, and according to IT staff at ADE, the plan has never been tested. The

An effective business continuity plan can help reduce the impact of a major IT service disruption.

plan is missing some key information, such as current contact information for key personnel, contact information for vendors, and information about alternate locations for command centers, backup sites, off-storage sites, and restoration sites. An effective business continuity plan reduces the likelihood and impact of a major IT service disruption on key organizational functions and processes.

Recommendations:

1. ADE should develop, adopt, and enforce the use of a single, effective agency-wide SLDC process.

2. ADE should create a plan to review current applications' technical and user documentation:

    a. Determine what needs improvement in order to maintain the applications;

    b. Address identified gaps; and

    c. Prioritize and schedule improvement activities.

3. ADE should identify, collect, and measure performance measurements for key IT functions and operations.

4. ADE should develop a plan and address resource requirements to allow it to perform regular risk assessments of its IT systems and operations, and should develop procedures to address issues raised.

5. ADE should fully develop a business continuity plan and should include provisions for regularly updating and testing the plan.

FINDING 4

ADE needs to ensure its information technology meets its business needs

ADE needs to take several actions to better ensure that its information technology efforts can meet its business needs. Information technology is key to many of ADE's administrative functions and responsibilities, but the IT section's staff are not included in the strategic planning processes of ADE or its divisions. This lack of coordination limits ADE's ability to ensure that initiatives will have the necessary IT support. Instead, key initiatives may languish, or ADE units may feel it necessary to develop IT applications on their own. Three things are needed: a steering committee to help guide information technology efforts, a review of whether the IT section is correctly positioned within the organization, and a more meaningful strategic planning process within the IT section itself.

Coordination of IT efforts limited

ADE uses information technology in many of its operations, such as collecting information for determining the amount of funding school districts and charter schools receive. Although ADE's strategic planning efforts are a primary way of helping the organization determine how best to meet its responsibilities, auditors found that IT considerations are not effectively integrated into these planning efforts. Better coordination involves both creating a coordinating mechanism and reassessing the IT section's place in the organizational structure.

ADE uses IT for many of its operations, but does not involve IT when developing goals that require IT efforts and resources.

ADE lacks key processes to help ensure IT meets business needs—

Two key ways to help ensure that IT efforts meet ADE's business needs are the agency's strategic planning efforts and its prioritization of IT initiatives. In both cases, there are problems:

- **Breakdowns in strategic planning efforts**—IT management or staff do not adequately participate in developing ADE's strategic plan despite the fact that IT resources may be needed to ensure objectives are met. For example, an

objective listed in ADE's strategic plan calls for the delivery of high-quality customer service by "increasing the use of data and information technology as a management tool to make better informed decisions."[1] However, IT was not involved in developing this objective, and the plan does not address how IT would meet this objective or the resources that are needed. Similarly, IT management or staff do not participate in the process that the divisions use to develop and implement their strategic planning goals. Divisions are assigned goals that have been developed by the Superintendent of Public Instruction, and ADE management is given the responsibility to ensure that related strategic plan objectives are developed and met. However, there is no process in place for effectively involving IT when the divisions develop goals for which IT efforts and resources are required. As a result, IT is frequently not involved with the division's planning efforts.

- No process for prioritizing IT initiatives—Further weakening ADE's ability to ensure that IT meets it business needs, ADE lacks a department-wide process for prioritizing IT initiatives and other efforts to ensure that agency-wide and division strategic goals are met. Rather, decisions such as how to prioritize IT projects or requests are often made by the IT section without input from ADE upper management and/or the affected divisions. While the IT section has some mechanisms for recording IT requests, IT management primarily determines how to prioritize those requests on its own.

Without a sufficient planning process in place, critical business needs may not be met.

Without sufficient planning processes in place, critical business needs may not be met or the divisions may feel it necessary to develop their IT applications without involving the IT section. For example, to avoid a reduction in federal funding for NCLB, the Academic Achievement division needs to develop an IT application that collects data on highly qualified teachers. This need has been brought to the IT section's attention; however, IT management believes that because of the lack of funding, it is unable to dedicate IT staff to develop and implement this application. In other instances, divisions or program units have hired their own programmers to obtain the applications they need. For example, the Exceptional Student Services (ESS) unit needed a new application to meet federal reporting requirements for special education services. As a result of this not being an IT priority, ESS reported that it hired its own programmer to develop this application.

ADE needs an IT steering committee to help establish IT priorities department-wide.

ADE should take steps to ensure that the IT section effectively meets ADE's business objectives—ADE needs to take at least two steps to ensure IT can effectively support its business goals and objectives. First, ADE should establish an IT steering committee that should include representatives from senior management, user management, and the IT function, such as the superintendent and/or deputy superintendent, the associate superintendents, the CIO, and other key ADE stakeholders, as appropriate. Best practice guidelines indicate that management and other key people who understand the business needs should be involved during the strategic planning process to help effectively communicate project goals to project teams and the value of IT to all stakeholders.

1 Arizona Department of Education Strategic Plan, fiscal years 2007-2011.

An IT steering committee helps to facilitate this communication and to better prioritize IT initiatives and projects on an organization-wide basis. This committee should ensure adequate IT involvement in the department and division planning processes. In addition, the committee should better direct the uses and allocation of IT resources (people, applications, technology, facilities, and data) throughout ADE. The committee should provide overall IT direction, help establish IT priorities department-wide, and ensure that adequate processes exist for identifying, funding, and allocating department-wide IT resource costs.

Second, ADE should consider whether the IT section's placement within the organization adequately ensures that IT can effectively meet ADE's business goals and objectives. The IT section reports to the Associate Superintendent of Education Policy, and therefore is three levels below the State Superintendent of Public Instruction, who is responsible for providing ADE's overall direction. Best practice guidelines indicate that the placement of the IT function in the overall organizational structure should be contingent on the importance of IT within the agency. Given IT's criticality, ADE should consider whether the IT section should be elevated within the organization. For example, in the Departments of Economic Security, Revenue, and Administration, the CIO is placed one level higher and reports directly to the deputy director.

IT section's planning process ineffective

The IT section's internal planning process is limited and ineffective. Therefore, ADE should ensure that the IT section effectively plans for ADE's current and future IT needs by having IT develop an effective planning process.

IT section lacks an effective planning process—The IT section's current internal planning process is very limited and does not identify the resources it needs to maintain and operate its current systems or plan for future IT initiatives. Further, IT management is unaware of how its plan integrates into ADE's strategic plan, and therefore has not ensured that its efforts are aligned with ADE's business needs.

The IT section's current plan was developed to comply with a statutory requirement that all agencies annually submit an IT strategic plan to GITA. As a result, the IT plan is focused primarily on the information required by GITA and does not address ADE's strategic objectives. In fact, according to the individual responsible for compiling the plan, the IT section did not solicit any stakeholder input from outside the IT section when it developed the plan. Further, the plan has remained virtually unchanged for the past 2 years and contains four objectives that are no longer applicable. For example, the fiscal year 2006 plan, which was finalized in September 2005, included objectives to organize and hold conferences/workshops on various topics related to the SAIS. However, effective in July 2005, the responsibility for this function was moved to the School Finance unit.

Agency IT plans facilitate the application of information technology to enable business initiatives, goals, and objectives of the budget unit in an efficient manner by describing a direction for current and future activities, supported by underlying principles, standards, and best practices

Source: Obtained from *GITA State-wide Policy*, p. 136.

ADE's IT plan process should include long-term IT direction and action plans for accomplishing goals and objectives.

ADE should ensure that the IT section develops an effective planning process—According to GITA standards, the IT section's planning process should define long-term IT direction that aligns with ADE's business needs, and include key stakeholders such as those who utilize IT services and information. Including key stakeholders will ensure that IT initiatives support ADE's mission and improve communication between IT and users on how their efforts will add value to their services. If ADE establishes the IT steering committee proposed earlier, this committee can provide the key stakeholder input for the IT section's plan.

Further, once a plan has been developed, strategies and steps to accomplish the plan are needed. The Governor's Office of Strategic Planning and Budgeting has developed components of an effective strategic planning process that specifically address the need to develop action plans to spell out the details and methods, or strategies, that will be used to accomplish the objectives, goals, and mission of the agency and its programs. To ensure that ADE's business needs are being met, IT management should develop an action plan that first formulates strategies; evaluates costs, benefits, and possible consequences of alternative courses of action; considers the resources needed; assigns responsibility for implementation; defines the steps that must be finished to complete the plan; sets a time frame for completion; and determines the resources necessary to carry it out.

Recommendations:

1. To ensure that IT can better meet ADE's mission and business needs, ADE should establish an IT steering committee that should include representatives from senior management, user management, and the IT function, such as the superintendent and/or deputy superintendent, the associate superintendents, the CIO, and other key ADE stakeholders as appropriate.

2. Once established, the ADE IT steering committee should:

    a. Ensure adequate IT involvement in the Department's and the divisions' planning processes;

    b. Provide overall IT direction for the Department; and

    c. Ensure that adequate processes exist for identifying priorities and funding, and allocating department-wide IT resource costs.

3. To ensure that IT can effectively meet ADE's business needs, ADE should review the IT section's organizational placement within ADE.

4. ADE should ensure that the IT section establishes an effective planning process which includes:

    a. Developing, with input from key stakeholders, an IT plan that defines the long-term direction that aligns with ADE's business needs; and

    b. Developing an action plan that first formulates strategies; evaluates costs, benefits, and possible consequences of alternative courses of action; considers the resources needed; assigns responsibility for implementation; defines the steps that must be finished to complete the plan; sets a time frame for completion; and determines the resources necessary to carry it out.

FINDING 5

ADE not in full compliance with student-level data collection notification and disposal requirements

During the audit, auditors also identified two areas in which ADE was not fully complying with statutory requirements. The first is a requirement that ADE tell school districts and charter schools the specific statutory authority for collecting each item of student-related data that ADE requires districts and schools to submit. ADE currently is not providing this information. The second is a requirement that ADE adopt guidelines to remove outdated student-level data collected by school districts and charter schools from SAIS. ADE has not done so, even though statute required it to adopt such guidelines by the beginning of the 2004-2005 school year.

ADE has not fully complied with student-level data collection requirements—A.R.S. §15-1042 establishes data submission requirements and timelines for SAIS. Subsection A of that statute requires ADE to "distribute a list of the specific student-level data elements that school districts and charter schools are required to submit." According to ADE, it has complied with this by providing a list of SAIS data elements on its Web site. However, subsection E further requires that "(e)ach student-level data element shall include a statutory reference to the law that necessitates its collection." During the course of this audit, auditors determined that while ADE publishes a list of the data elements contained in SAIS, it does not include information on the statutory reference requiring its collection. Instead, it includes information on whether the data elements are required by the state or federal government. In order to fully comply with the law, ADE should publish in one document both the specific student-level data elements that it collects and the statutory reference requiring their collection. Additionally, while there may be other data elements collected for which there is no specific statutory reference, but nevertheless are important in order for SAIS to operate effectively, ADE should also include those elements in its list and could cite the reference for the process that ADE must perform, or otherwise describe how the data fills a need in the process in order to make SAIS complete. According to ADE, it has begun to compile this information and anticipates it will be publishable by the middle of fiscal year 2007. ADE should finish compiling the list of data elements

ADE needs to publish a list of student-level data elements that includes a statutory reference to the law necessitating collection.

collected through SAIS and establish a deadline to publish the information no later than the end of fiscal year 2007.

ADE has not adopted guidelines to remove outdated SAIS student data—A.R.S. §15-1042(I) also requires ADE to "adopt guidelines to remove outdated student level data collected by school districts and charter schools from the student accountability information system beginning in the 2004-2005 school year." Although the Legislature added this requirement in 2003, ADE has not yet adopted any guidelines to comply with this requirement. ADE explains that it has not adopted guidelines because changes in state and national education data collection trends, including initiatives from the U.S. Department of Education and Arizona's Governor, suggest that ADE may need education data for longer periods of time than statute currently allows. However, it appears that statute does not prescribe a retention period for student-level data. Therefore, ADE should adopt a retention schedule for such data and adopt guidelines to remove the outdated data in SAIS in accordance with state statute.

Since statute does not prescribe a retention schedule for student-level data, ADE should adopt one.

Recommendations:

1. ADE should finish compiling the list of data elements that it collects through SAIS and should:

    a. Include references to the statutory authority for gathering each piece of information, as required by A.R.S. §15-1042(E);

    b. Include in its list other data elements collected for which there is no specific statutory reference and cite the reference for the process that ADE must perform, or otherwise describe how the data fills a need in the process in order to make SAIS complete; and

    c. Establish a deadline to publish the information no later than by the end of fiscal year 2007.

2. ADE should adopt a retention schedule and guidelines to remove outdated student data from SAIS.

GLOSSARY

Access Log—A file containing a list of the requests or actions that computer users take or make on a computer system or device. Sometimes referred to as "raw data," access logs can often be analyzed and summarized by another program to identify anomalies and/or trends.

Authentication—The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Authorization generally follows authentication.

Authorization—The process of granting access to a user and allowing him/her to use the pre-approved resources in the system, and the privileges of use (such as access to file directories, hours of access, amount of allocated storage space, etc.). Authorization is preceded by authentication.

Capacity Management—The ability to monitor and measure in real time the performance of a computer environment and to forecast its future usage. Used to determine the system capacity needed to deliver specific operational and performance levels through quantification and analysis of present and projected workloads.

Configuration—The way a system is set up, or the assortment of components that make up the system. Configuration can refer to either hardware or software, or the combination of both. When you install a new device or program, you sometimes need to configure it, which means to set various switches and jumpers (for hardware) and to define values of parameters (for software).

Cookie—A small text file of information that certain Web sites attach to a user's hard drive while the user is browsing the Web site. A cookie can contain information such as user ID, user preferences, archive shopping cart information, etc. Cookies can sometime contain personally identifiable information.

Database—A collection of electronic information organized in such a way that a computer program can quickly select and/or process desired pieces of data. A database is commonly thought of as an electronic filing system.

Glossary (cont'd)

Debugger—A special program used to identify coding errors or problems (bugs) in other programs. A debugger allows a programmer to stop a program at any point and examine and change the values of variables.

Encryption—The translation of data into a secret code that is typically not in a humanly readable form. Encryption is often an effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

Hacker—A slang term for a computer enthusiast who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). The negative connotation of hacker refers to individuals who gain unauthorized access to computer systems to steal data and/or to carry out other ill-intended purposes.

Intranet—A private, internal Web site belonging to an organization and generally only accessible by an organization's members, employees, or others with authorization.

Malicious Code—Program code added, changed, or removed from a software system in order to intentionally cause harm, perform unauthorized activities, or use up resources of a computer or information system. Three typical types are as follows:

- **Virus**—A program which, when executed, can add itself to other programs without permission and in such a way that the infected program, when executed, can cause ill-intended actions to occur or add itself to still other programs.

- **Worm**—A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message.

- **Trojan**—A program that masquerades as a legitimate program, but does something other than what was intended.

Media Sanitization—The process of removing data from electronic storage media such that data recovery using known techniques is prevented. It is intended to provide reasonable assurance, in proportion to the confidentiality of the data, that the data may not be retrieved and reconstructed.

Mobile Devices—Small, portable computing devices that allow users to store, organize, and access a variety of information. They are typically powered by batteries and need to be charged for use. They range in size from a stack of business cards to a paperback book. Typical examples of mobile devices include Personal Digital Assistants (PDA), cell phones, and laptop computers.

Glossary (concl'd)

Script—A computer program or a sequence of instructions that are interpreted by another program. A script is normally used to automate routine, complex, or advanced features or procedures within a system. Scripts are commonly used to process user information from Web pages.

Security Patch—Piece of software code that can be applied after a software program has been installed to correct an issue(s)—specifically related to the prevention of, or protection against, access to information or systems by unauthorized recipients, and intentional but unauthorized destruction or alteration of that information—with the original program. This can range from fixing software bugs to improving the usability or performance of a previous version of a program.

Vulnerability—A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. These weaknesses could be exploited to gain unauthorized access to information or disrupt critical processing.

Vulnerability Scanning—A preventive measure to deter attacks against the system by identifying weaknesses before they can be exploited. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws, and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Web Server—A computer that hosts a Web site. It delivers requested Web pages and sends them to a user's Web browser for display. It provides services to clients on the network such as Web-based applications.

Web-based Application—A software program or system that is accessed with a Web browser, such as Internet Explorer, over a network such as the Internet or an intranet. Software components usually reside on a Web server and generally only need to be installed on one machine. This provides the ability to update and maintain Web applications without distributing and installing software on potentially thousands of client computers and is a key reason for their popularity.

AGENCY RESPONSE

State of Arizona
Department of Education

Tom Horne
Superintendent of
Public Instruction

August 11 , 2006

Ms. Debra K. Davenport, CPA
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85010

Dear Ms. Davenport:

The Arizona Department of Education is providing the enclosed response to the Auditor General's performance audit for the following area:

- Information Management Function

We appreciate your work on this performance audit, your consideration of our previous comments and suggestions and your acknowledgement of the quality and variety of work already provided by the Arizona Department of Education.

Please feel free to call me at (602) 364-2339 if any additional information is needed.

Sincerely,

Margaret Garcia Dugan
Deputy Superintendent

Enclosure

Arizona Department of Education (ADE)

Response to Auditor General's Performance Audit on Information Management August 11, 2006

Introduction

Superintendent Horne decided before this audit began that ADE's Information Management function required attention. Starting with ADE's Management Information Systems (MIS) section – and coincident with the start of the Information Management Performance Audit – in mid-September of 2005 Mr. Horne made a significant management change to the technology organization, appointing a new Chief Information Officer (CIO). Charged with bringing the section in line with agency needs and industry standards, and given authority to institute across-the-board changes to achieve that goal, the new CIO spent the last nine months modernizing and "professionalizing" the renamed Information Technology (IT) section. With the assistance of the information learned from this audit, ADE's IT section has been able to fast-track implementing plans to move the section from a production shop to a mature standards-based service-oriented IT organization.

- We have worked with an independent technology strategy consultant and with the Arizona Auditor General's office to discover the former MIS section's many gaps and to incorporate acceptable standards into the new IT organization: procedures, processes, and practices for all aspects of IT, such as strategic planning, project management, software development, product delivery, quality assurance, operations, configuration management, etc.
- New project development standards require early and continued collaboration with stakeholders, both internal and external to ADE.
- We have implemented upgrades and realignments to our network, software, and hardware environments, speeding processing windows of applications, such as some SAIS processes by 400% to 800%.
- A stronger emphasis is now placed on service delivery to schools and districts/charter holders – referred to as local education agencies (LEAs) in the education community. ADE actively participates in LEA technology forums, and works collaboratively with LEAs on new ADE technology initiatives. ADE has taken steps to support technology platforms used by the LEAs so that student-based technology decisions will no longer be hampered by constraints of ADE's business system delivery methods.

We're well on our way with the changes, and the IT staff has embraced the new vision. This "modernization" period has shown that ADE's greatest technological asset has been the existing IT staff itself. The IT section has been fortunate enough to meet the challenge of economically hiring experienced IT professionals who come to the table with great depth of experience and long history in standards-based, procedure-driven IT organizations, despite IT's constraints of equally modest operating and training budgets. Existing staff have enthusiastically contributed their expertise to designing and implementing the new suite of procedures, processes, and practices governing the IT section.

Last but not least, the Arizona Auditor General's office has been most generous in sharing their expertise with regard to the changes being made at ADE. While not recommending solutions, they have reviewed plans and given advice regarding thoroughness, fit, and industry best practices where appropriate. Their suggestions and guidance have enabled ADE to move much more swiftly and confidently along the path of improvement.

Audit Finding 1: ADE needs to better manage security of its information technology systems and operations

Audit Recommendations:

1. *ADE should develop and implement an ongoing process for addressing IT security vulnerabilities or control weaknesses when they are discovered. The process should ensure that known security concerns are evaluated and prioritized in order of risk, that specific plans to address them are developed, and that responsibility for correcting them is assigned.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

2. *ADE should identify specific security objectives, assess its current set of policies and procedures against those objectives, analyze any gaps, consider the risk associated with each, develop a plan to implement effective policies and procedures, and monitor them on a regular basis.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

3. *ADE should develop a process to identify and implement specific security guidelines for its systems, incorporate them within its systems development and testing process, and train its development and testing staff on security concerns and methods.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

4. *ADE should consider creating an appropriate position to be responsible for all IT security within ADE. The reporting line of the security position should be such that it can effectively design, implement, and enforce compliance with the organization's security policies, standards, and procedures, and ensure that they are functioning effectively.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.[1]

[1] Achieving this objective requires that sufficient additional staff and funding are secured in a timely manner.

ADE Corrective Actions:

Overall ADE IT Security Corrective Action Plan:

During the span of the auditor's field work the newly appointed leadership of Arizona Department of Education's (ADE) Information Technology (IT) section launched an agency-wide initiative dedicated to leading the agency toward the objectives associated with the development, purchase, maintenance and operation of trusted, dependable applications. ADE IT recognized the need to identify and classify technological assets requiring protection to provide a focus on security risks. Areas of concentration include data assets, managed applications, operations, development and maintenance processes, network assets, data transport mechanisms, third party application management and monitoring.

As a result of the importance of these requirements, Superintendent Horne empowered ADE IT to set aside other agency priorities to focus upon securing the agency's technical assets with an initial emphasis on identified critical web based applications. The resulting initiatives have provided ADE IT with the opportunity to develop and implement the repeatable processes required to assure ADE's applications are certified secure and have the native agility to react to the continual onslaught of new threats. The objectives of this strategy included:

1. Determining the roles and responsibilities of management, technical staff, business units and users. Establishing procedures for creating accounts and passwords and maintaining user access and then monitoring departments for compliance.
2. Creating policies for privacy and confidential data storage including the stratification of data from sensitivity and security perspectives into specific classifications. Documenting how locally stored information is stored, used, and transmitted, archived and how to best protect this information.
3. Creating a physical security plan that manages access to all workspaces.
4. Creating network configuration and segmentation plans.
5. Implementing an agency and state level coordinated business continuity plan.
6. Establishing change control processes which prevent implementation of fixes or changes to production code without proper analysis and documentation of requested changes.
7. Creating a process for keeping third party software up to date through a managed patching strategy.
8. Providing a software licensing policy which mandates only use of software that is licensed to use and conduct audits.
9. Providing a methodology for user awareness training and require all employees to read, commit to following, and sign off on security guidelines on an annual basis.
10. Improving network based security access methodologies.
11. Ensuring that Anti Virus software is installed and successfully functioning on all technical assets.
12. Providing helpdesk and other support staff security training.
13. Developing an inventory of ADE managed applications including the evaluation of security and business process risk assessments.

14. Limiting development of enterprise-level applications to the IT staff only, and permitting access to enterprise-level development-related assets and environments only to IT staff.

The resultant completed documented guidelines and processes have been wrapped in an internal program designated "ADE IT's Services Management" and have been widely disseminated. They include:

1. Application development management.
2. Operations management.
3. Problem and issue management.
4. Change management.
5. Release management.
6. Security management.
7. Organizational roles and responsibilities (including users and business units).
8. Document management.
9. Configuration management.
10. Business continuity and disaster recovery management.
11. Enterprise data management.
12. IT project financial management.
13. Application testing functional and security certification management (testing applications for application functionality and for conformance with security standards).

Guidelines detailing ADE IT's plans for user acceptance testing and communication methodologies and ongoing professional development relating to IT security are still in the process of authorship.

Creation of these guidelines and processes has no value unless the organizational taxonomy and culture can accept these directives as the ultimate way of doing business. To that end, the formation of groups empowered to create and enforce agency IT standards – groups such as IT data management, project management, IT operations, an IT security review board, an IT operations steering committee, and an application migration gate review board – bring relevance and value to the documented guidelines and processes listed above in the day-to-day tactical events of each IT team member. Finally, the processes include the systematic reevaluation of the ADE-authored guidelines, created processes and formulated teams so their individual effectiveness can be determined and adjustments can be made.

With regard to the auditor's fourth recommendation ADE fully acknowledges the need to create a position directly responsible and accountable for ADE IT security. As a result, a request for the funds is being made to the Legislature in a supplemental budget request so that ADE can immediately fill this FTE position. ADE is also submitting an FY2008 decision package for funding for additional IT security staff.

Audit Finding 2: ADE can further enhance SAIS' reliability

Audit Recommendations:

1. *To improve SAIS data reliability, ADE should implement additional controls. Specifically, ADE should:*
    a. *Establish a department-wide comprehensive procedure for developing and implementing business rules.*
    b. *Implement automated variance checks by identifying appropriate staff to determine what types of variance checks should be added, as well as assigning responsibility for following up on any data variances that appear unreasonable.*
    c. *Add processing controls such as run-to-run totals and data reconciliation, and review information collected from the controls at least twice a month to help prevent potential problems with SAIS data.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

2. *To help improve SAIS' functionality, ADE should:*
    a. *Obtain user acceptance of the one report that has been developed for archiving.*
    b. *Develop and implement other SAIS archived reports.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

3. *To address user concerns and identify additional ways to improve SAIS, ADE should:*
    a. *Establish a tactical team composed of representatives from ADE's IT section, and both internal and external stakeholders to identify and prioritize its user community's needs.*
    b. *Establish a schedule for implementing the agreed-upon SAIS changes.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

4. *To improve SMS software performance, ADE should:*
    a. *Ensure the SAIS SMS software test environment is up to date and available when needed.*
    b. *Monitor software performance and take steps to address any problems identified.*
    c. *Consider establishing a recurring SMS software certification or rating process.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.[2]

[2] Achieving this objective requires that sufficient additional staff and funding are secured in a timely manner.

ADE Corrective Actions:

ADE is taking the following steps toward reducing the quantity of SAIS transaction failures:

- IT will expand existing system validation mechanisms aggressively to reduce transaction errors caused by incorrect student management system (SMS) functionality. The program will entail testing of vendor SMS software, and formal certification granted for every SMS vendor feature.
- ADE maintains a continuing effort to reduce transaction failures caused by system errors, even though the number may be minimal.
- Migration to the storage area network (SAN), with the increased number and size of servers running SAIS (December 2005-January 2006), has already improved processing times and has reduced system errors.
- ADE's School Finance STaR team, in its capacity of providing SAIS training, is in a prime position to identify areas of challenge for users with their SMSs, and thereby aid users in anticipating problems and further minimizing data entry errors.

The implementation of the software development life cycle (SDLC) and a formal change control process will ensure that ADE has a comprehensive procedure for developing and implementing business rules.

Even though the audit survey showed mostly positive results, ADE nonetheless wishes to further investigate the issues that the survey identified, as some of the reported issues had not previously been reported to ADE. However, because the Auditor General's office promised confidentiality to all survey respondents, ADE cannot contact these users directly. ADE has many ways of collecting information from users regarding SAIS, for example: through the ADE Support Center, email to ADE, and User Meetings. However, in order to reach users that responded to the survey with issues, ADE will broadcast a request to SAIS users, inviting them to provide detailed information about issues they may have. In that way these issues can be analyzed, addressed, and resolved.

When SAIS was first developed, a rigorous testing program was set up between ADE and SMS vendors. Unfortunately, however, lack of resources and financing after year 1 of SAIS forced ADE to reduce the interaction with the vendors. Once funding and resources are made available, ADE is eager to resume and expand the program to work more closely with all vendors that provide interfaces to SAIS. The program will include annual testing to ensure that vendor software is up-to-date; that it operates according to published business rules; and that the vendor testing site remains available. Monitoring and publicly reporting results of testing on the various available SMS software will be ongoing throughout the school year.

The IT section developed the capability to archive a key student level funding report. This function will be fully implemented, pending internal ADE user sign-off, as urged in the Audit Report. The goal is to have this and many more reports available in archived form. Following the accomplishment of this, IT will need the advice and recommendations of SAIS stakeholders to determine which other reports should be available for archiving.

ADE is working to improve our methodologies to improve communication and interaction with all SAIS users. The Audit Report acknowledges the existence of the current SAIS Stakeholders group facilitated by the School Finance System Training and Response (STaR) team, and that the group coordinates the interests of ADE unit staff who work with SAIS, but STaR does not coordinate the interests of the IT staff. The group is a valuable user group comprising great depth of local expertise across many agency units; the group coordinates SAIS operational issues such as cross-unit calendar requirements. The IT section is creating a new tactical team that can identify

and prioritize SAIS needs, as presented in one of the Audit Report's recommendations. This SAIS tactical team will be driven by the new IT project initiation and change management procedures to ensure that appropriate business rules are completely and successfully implemented. The SAIS tactical team will identify a designated user group – quite possibly the School Finance STaR team's SAIS Stakeholders group – to be involved in all user steps such as requirements identification and testing processes.

Audit Finding 3: ADE needs to improve IT project management and operations oversight

Audit Recommendations:

1. *ADE should develop, adopt, and enforce the use of a single, effective agency-wide SDLC process.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

2. *ADE should create a plan to review current applications' technical and user documentation:*

    a. *Determine what needs improvement in order to maintain the applications.*

    b. *Address identified gaps.*

    c. *Prioritize and schedule improvement activities.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.[3]

3. *The ADE should identify, collect, and measure performance measurements for key IT functions and operations.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

4. *ADE should develop a plan and address resources requirements to allow it to perform regular risk assessments of its IT systems and operations, and should develop procedures to address issues raised.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.[4]

5. *ADE should fully develop a business continuity plan and should include provisions for regularly updating and testing the plan.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.[5]

[3] Achieving this objective requires that sufficient additional staff and funding are secured in a timely manner.
[4] Achieving this objective requires that sufficient additional staff and funding are secured in a timely manner.
[5] Achieving this objective requires that sufficient additional staff and funding are secured in a timely manner.

ADE Corrective Actions:

IT Project Management

The IT section has made great strides toward improving project management. Eighteen months ago, there was no central project management, and no standard approach to handling projects. Early in 2005, prior to commencement of the IT performance audit, the IT section recognized the need for more effective, structured procedures. A project management office (PMO) was instituted, with its director to be a certified project management professional (PMP®), reporting directly to ADE's Chief Information Officer. IT's project management office has been fully established since late 2005, is headed by a certified PMP, and staffing will be completed with professional project managers. The PMO director has instituted formal project management and reporting procedures that are aligned with SDLC standards. The software development process is being expanded and improved on an ongoing basis, with early emphasis placed on stakeholder communication, integration of security, and documentation templates. This formal SDLC-aligned process has been widely disseminated within ADE, and all future IT projects will conform, whether they are developed by IT staff or by staff in another ADE section. The PMO, with its director and its project managers, will maintain central oversight of the entire agency's IT projects. The IT section has made great strides, and will continue to improve upon the progress that has already been made.

Documentation

The IT section has long recognized the need for improvement in IT documentation at every level – requirements, specifications, architecture, detailed design, testing/Quality Assurance, user, etc. IT suffers from the same dilemma as most other technology organizations – having inadequate resources to accomplish all of its responsibilities. This dilemma results in a choice between two poor options: Option A, create all required documentation for an application but remain unable to deliver complete functionality); or Option B, deliver a functional application but fall short in documentation. Historically, IT and the agency have consistently chosen Option B, but with the new institution and enforcement of SDLC procedures, ADE is committed to delivering both functional applications and complete documentation.

Oversight/Performance Measurement

Last year's appointment of a new CIO, reordering of the IT organizational structure[6], creation of the IT operations team, and securing the services of a consulting Technology Strategist who modeled the role for a new Chief Technology Officer (CTO) position, have brought greater focus and expanded coordination within the IT section. Application developers, for instance, are now able to concentrate their efforts strictly upon their own areas. They will no longer be diverted from their tasks, as regularly occurred in the past, to perform operations, testing, or business analysis. IT has established service level objectives (SLO), and is on its way to establishing Key Performance Indicators (KPI), helping to define and measure progress toward the agency's IT goals. The end result is that IT staff members are now in a far better position to apply performance measures and quantify the results of those functions and operations that are essential for serving IT's customers and carrying out its mission.

Oversight/Risk Assessment and Mitigation

In May and June of 2006, ADE conducted a rigorous IT risk assessment. This is now being followed by ongoing periodic risk assessments as we move forward. The initial assessment required a full two months, during which time a moratorium on new development enabled 100% of IT staff members to dedicate their efforts to risk assessment and mitigation – a massive, consolidated ef-

[6] See attached organizational chart.

fort of over 17,000 man-hours. The end result is that all critical ADE applications have been tested for security weaknesses, and both individual and systemic weaknesses were mitigated. Risk assessment is now standard operating procedure, ensuring that all future applications will have the same attention before their implementation.

The reordering of the IT section included a clear definition of roles and responsibilities, and new documentation procedures that now capture application details (both business and technical), significantly reducing the risk of service interruption as a result of the departure of an employee.

Oversight/Business Continuity

ADE understands the need to ensure that its business will continue with minimal interruption, should the agency be faced with a disaster, whether natural or human-caused. IT participates in the governor's statewide disaster recovery program, and has sought assistance from the Government Information Technology Agency (GITA) to aid in establishing an effective action program for ADE. Applying GITA's advice, IT formulated its initial plan for data recovery from backup tapes. Following GITA's review and response, IT managers met with GITA's security technology manager for further discussion, and IT's Director of Network Services & Infrastructure participated in a training seminar covering disaster recovery, business continuity, and backup restoration. IT will apply GITA advice and knowledge gained from the disaster recovery training seminar, revise the initial plan and resubmit to GITA. Following GITA approval, the plan will be implemented.

Audit Finding 4: ADE needs to ensure its information technology meets its business needs

Audit Recommendations:

1. *Establish an ADE IT steering committee.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

2. *Ensure IT involvement in department planning, provide overall ADE IT direction, ensure processes exist for prioritizing, funding, and allocating IT resource costs.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

3. *To ensure that IT can effectively meet ADE's business needs, review the IT section's organizational placement within ADE.*

The finding of the Auditor General is not agreed to and the recommendation will not be implemented.

4. *IT section should establish an effective planning process.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

ADE Corrective Actions:

ADE discovered before this audit began that its IT section had indeed been operating with an ineffective planning process and that IT was underrepresented in the agency's strategic planning efforts. Superintendent Horne immediately embarked on an encompassing set of remedies. In the Fall of 2005 ADE's new CIO was charged with transforming the IT section from a production shop to a service-oriented organization driven by industry-standard methodologies. The new CIO was added to the Executive Team for closer exposure to all ADE divisions at the Executive level. Plans for a new IT Executive Steering Committee which will prioritize IT projects and initiatives were discussed with the Executive Team in February 2006; the group will begin its hands-on work in the Fall of 2006. Beginning in the FY2008 planning cycle, the IT section will be included in each division's strategic planning process.

IT Executive Steering Committee

The new IT Executive Steering Committee will commence operation in the Fall of 2006. It will be comprised of the Deputy Superintendent, all Associate Superintendents, and the CIO. Other key ADE stakeholders will be invited as the project requests require. This IT Executive Steering Committee will drive prioritization of IT projects, will ensure that IT direction is aligned with agency-wide goals, will involve IT in agency-wide technology planning, and will commit on behalf of all divisions to adopt and enforce adherence to IT's policies, procedures, and practices.

With IT's new SDLC ADE IT has implemented a broad suite of standard policies, procedures, and practices. These support and expand upon previous lightly-documented methods in place for managing system issues and bug fixes. This new suite– such as procedures governing requests for new project initiation and system/application changes – gives IT, the ADE divisions, and the IT Executive Steering Committee the tools necessary to manage and anticipate demand for IT services.

Agency-wide Technology Planning

A primary objective for the IT Executive Steering Committee is commitment to involve IT in agency-wide technology planning, the only way to ensure ADE's ability to have IT meet its business needs in the short term and as well as in the long term. As stated earlier, beginning in the FY2008 planning cycle, the IT section will be included in each division's strategic planning process.

The IT Executive Steering Committee will review not only IT projects but also all technology projects taking place at ADE that are not provided by the IT section. This will enable the IT Executive Steering Committee to gain an overall picture of the technology needs of the agency, to control technology redundancy and inefficiency, and to assure appropriate application of data and technology resources at the agency.

Adherence to these new procedures will give the IT Executive Steering Committee the tools necessary to enable it to provide overall IT direction for the Department.

Organizational and Physical Placement of ADE-IT

The IT section's placement in the ADE organization will remain unchanged. Agency management from the Deputy Superintendent down to the Deputy Associate Superintendent level is given the opportunity to decide by consensus on commitment to enforce IT policies, procedures, and initiatives on a case-by-case basis. This strategy has proven to be effective in terms of buy-in from divisions, sections, and units on the way information is managed at the agency.

IT's physical placement, however, will change. Based on guidance from the Auditor General's office, the IT section will move to the main ADE building at 1535 West Jefferson Street to be co-

located with its major internal users. Close physical proximity enhances teams' effectiveness by providing more and easier opportunities for communication and collaboration.

IT Planning

The IT section is implementing steps to improve its internal planning process. In February 2006 we began requiring industry-standard formal project planning materials – including justification, documented requirements, cost estimates, etc. – for new projects and enhancement requests. These standard materials are an integral part of the foundation for IT's ability to plan effectively. Convoluted rules involving allocation of resources to state versus federal projects make the planning process extremely challenging but not impossible. ADE is evaluating a new resource allocation planning methodology for practical workability in the state education agency arena.

ADE's current CIO has placed a higher priority on participating in GITA's CIO Council group. This participation has positioned ADE's IT section to build partnerships with other state agencies, fostering dialogues that have assisted ADE in moving toward creating more meaningful, stronger IT operational and strategic plans. The IT section has begun steps to synchronize the various strategic planning efforts in which it is involved (ADE, GITA, OSPB, U.S. Department of Education, AZ Governor's Office, etc.), to transform them from required deliverables into useful management tools.

Audit Finding 5: ADE is not in full compliance with student-level data collection notification and disposal requirements

Audit Recommendations:

1. *Compile and publish by 6-30-2007 a list of SAIS data elements and the statutory authority for gathering each element.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

2. *Adopt a retention schedule and guidelines to remove outdated student data from SAIS.*

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

ADE Corrective Actions:

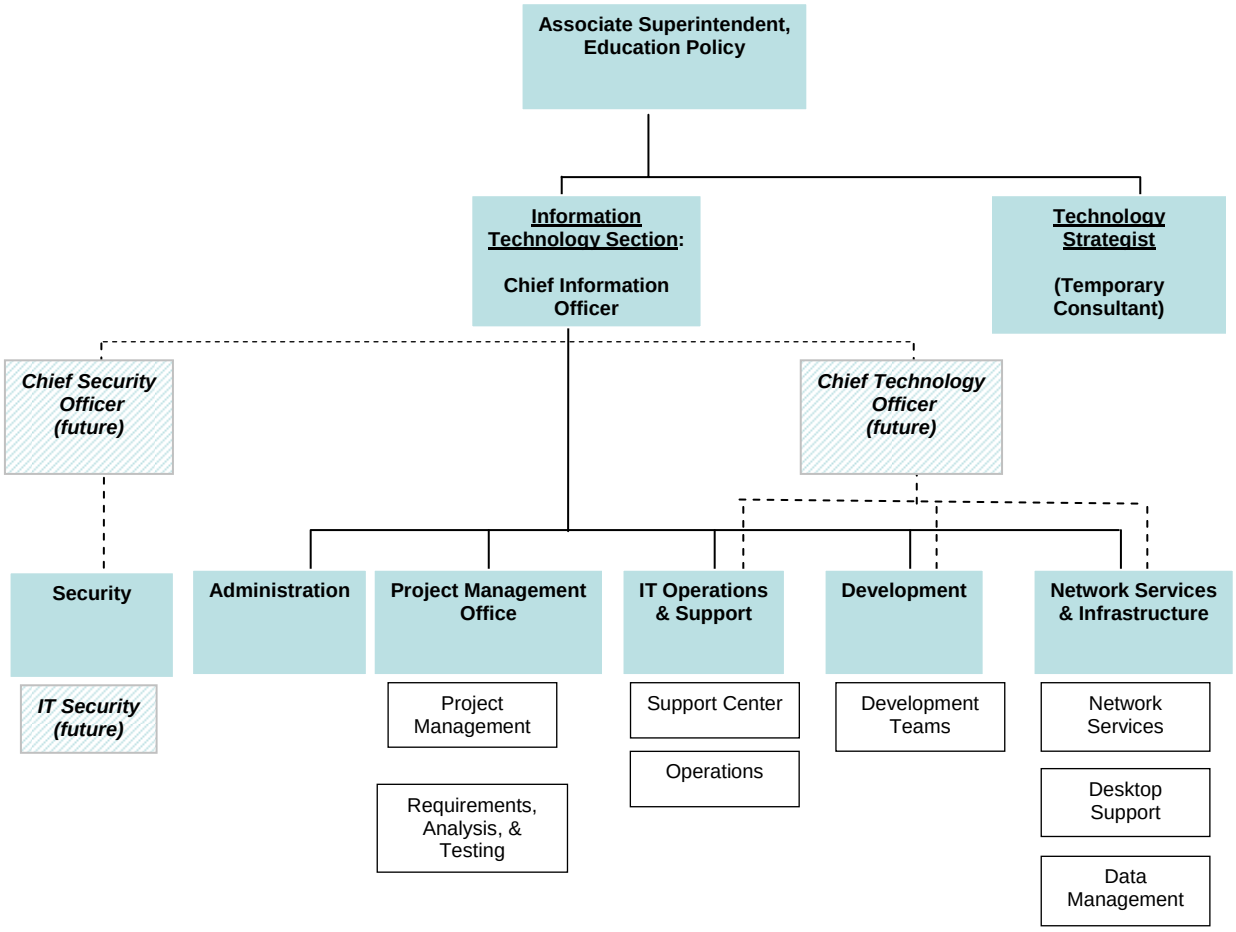
Failure to meet these statutory requirements was an oversight on ADE's part, and has already been remedied. These items have been completed and posted on ADE's website, at http://www.azed.gov/sais/.

Glossary

ADE.....Arizona Department of Education
CIO.....chief information officer
CSO.....chief security officer
CTO.....chief technical officer
FTE.....full time equivalency
FY.....fiscal year
GITA.....Government Information Technology Agency
HR.....Human Resources
IT.....Information Technology
KPI.....Key Performance Indicators
LEA.....Local Education Agency
MIS.....Management Information Systems
OSPB.....Office of Strategic Planning and Budgeting
PMO.....project management office
PMP® .....certified project management professional
QA.....quality assurance
SAIS.....Student Accountability Information System
SAN.....storage area network
SDLC.....software development life cycle
SLO.....service level objectives
SMS.....student management system
STaR.....Systems Training and Response
USDOE.....U.S. Department of Education

ADE IT Organizational Chart

The following organizational chart shows the current IT organizational structure as of July 1, 2006. It also reflects future staffing required to progress agency IT initiatives identified during the recent IT reorganization and during the Auditor General's audit.



Performance Audit Division reports issued within the last 24 months

04-07 Department of Environmental Quality—Air Quality Division
04-08 Department of Environmental Quality—Sunset Factors
04-09 Arizona Department of Transportation, Motor Vehicle Division— State Revenue Collection Functions
04-10 Arizona Department of Transportation, Motor Vehicle Division—Information Security and E-government Services
04-11 Arizona Department of Transportation, Motor Vehicle Division—Sunset Factors
04-12 Board of Examiners of Nursing Care Institution Administrators and Assisted Living Facility Managers
05-L1 Letter Report—Department of Health Services—Ultrasound Reviews
05-01 Department of Economic Security—Division of Employment and Rehabilitation Services—Unemployment Insurance Program
05-02 Department of Administration—Financial Services Division
05-03 Government Information Technology Agency (GITA) & Information Technology Authorization Committee (ITAC)
05-04 Department of Economic Security—Information Security
05-05 Department of Economic Security—Service Integration Initiative
05-06 Department of Revenue—Audit Division
05-07 Department of Economic Security—Division of Developmental Disabilities
05-08 Department of Economic Security—Sunset Factors
05-09 Arizona State Retirement System
05-10 Foster Care Review Board
05-11 Department of Administration—Information Services Division and Telecommunications Program Office
05-12 Department of Administration—Human Resources Division
05-13 Department of Administration—Sunset Factors
05-14 Department of Revenue—Collections Division
05-15 Department of Revenue—Business Reengineering/ Integrated Tax System
05-16 Department of Revenue Sunset Factors
06-01 Governor's Regulatory Review Council
06-02 Arizona Health Care Cost Containment System—Healthcare Group Program
06-03 Pinal County Transportation Excise Tax
06-04 Arizona Department of Eduation—Accountability Programs
06-05 Arizona Department of Transportation—Aspects of Construction Management
06-06 Arizona Department of Education—Administration and Allocation of Funds

Future Performance Audit Division reports

Arizona Department of Health Services—Behavioral Health Services for Adults with Serious mental Illness in Maricopa County

Arizona Supreme Court, Administrative Office of the Courts—Information Technology and FARE Program