STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

INTEGRITY • ACCOUNTABILITY • MAKING A DIFFERENCE

Department of Education
Information Management

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Subject

Information technology (IT) is critical to the Department of Education's (ADE) ability to manage and track the expenditure of state and federal funds; collect and report on information about students, teachers, and schools; and perform its other functions.

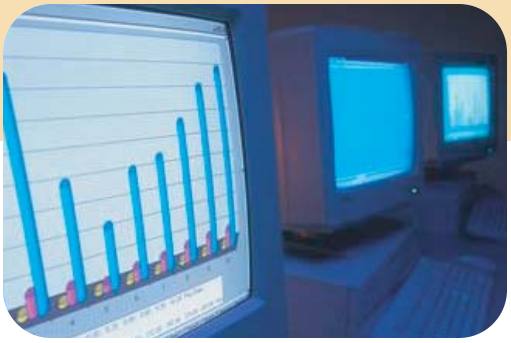
Our Conclusion

Improvements are needed in all IT areas we examined. The most critical need is for improved IT security. ADE also needs to improve the Student Accountability Information System's (SAIS) reliability, which is used for calculating school funding. Further, ADE needs a more structured approach for developing and maintaining IT systems and to improve its planning and prioritization of its IT resources.

2006

August • Report No. 06 – 07

ADE Needs To Better Manage IT Security



Sensitive information—such as students' names and birthdates and teachers' social security numbers—has not been adequately safeguarded because of security weaknesses in ADE's computer applications. ADE has 76 active Web-based applications (accessed from the Internet and through its internal network), which it uses to collect and report on information about students, teachers, and schools in Arizona.

About 3,300 different organizations and more than 13,600 individual user accounts have access to at least one of ADE's Web-based applications.

All 12 applications reviewed are vulnerable—We hired an independent consulting firm to help us assess the security of 12 ADE Web-based applications. The applications reviewed included those that are most frequently used and contain the most sensitive information, such as student and teacher personal information. Although auditors found no indication that such information had been compromised, the review found multiple vulnerabilities in all 12 of the applications. During the course of our 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.

ADE needs to improve its security practices—ADE also does not follow critical security practices. Auditors reviewed 13 significant IT security objectives, including:

- Monitoring user activity to detect unauthorized access or abnormal activity;
- Identifying and installing security updates; and
- Monitoring its IT systems to detect intrusions.

Although ADE has policies or procedures for many important security objectives, auditors found that for 12 of the 13 areas reviewed, the policies or procedures need to be improved.

Some known problems not addressed—ADE had external security reviews in 2002 and 2004, which identified a number of potentially serious weaknesses. It has also identified additional security weaknesses on its own. However, ADE indicates that for many of these weaknesses, corrective action is either in progress or it lacks adequate resources to implement a corrective action plan.

ADE should consider creating an IT security position—ADE should consider assigning an employee specific responsibility for agency-wide IT security and ensure there is a coordinated approach for identifying and addressing security weaknesses.

Recommendations

ADE should:

- Develop and implement an ongoing process for addressing security weaknesses when they are discovered;
- Develop effective policies and procedures to ensure good security practices are followed; and
- Consider establishing an agency-wide IT security position.

ADE Needs To Improve SAIS Reliability

SAIS collects and processes student data to determine funding and academic performance. The data comes from more than 700 districts and charter schools who use Student Management System (SMS) software to transmit data to SAIS. In FY 2006, 46.5 million transactions were submitted to SAIS. Nine percent of these transactions failed. Failures can result from bad data, software problems, or SAIS system failures. As such, SAIS' success requires cooperation from all parties involved.

SAIS Processing Data
Fiscal Year 2006

- 46.5 million transactions
- 4 million failed transactions
- 145,000 failed transactions because of system error
- 91 percent overall transaction success rate

Concerns about data accuracy—Although the majority of SAIS users auditors surveyed have confidence in SAIS data accuracy, some concerns were found. Over one-third of 338 SAIS users surveyed reported that they had experienced problems with data being dropped or disappearing from SAIS. Approximately 29 percent of the survey respondents were not confident that the data was accurate for final reporting or funding purposes.

Concerns about resources—Problems working with SAIS cost both time and money. One survey respondent who works for districts reported that SAIS has increased administrative costs at a time when they are under pressure to lower administrative costs.

Improving reliability of SAIS data—One step toward more reliable data would be to further improve processing controls. Some controls—such as those that ensure data files are the right size—are in place. However, automated variance checks are absent altogether and should be implemented.

Variance checks call attention to unusual differences in data.

Improving functionality—ADE can improve SAIS' functionality using minimum resources. ADE should continue its efforts to archive SAIS reports so that users can more easily reconcile data when a problem is suspected. ADE should also establish a tactical team to identify and address other concerns SAIS stakeholders may have.

Improve oversight of school software—Districts and schools use SMS software to record and process data and then submit it to SAIS. There are at least 20 different SMS packages. The packages have error rates ranging from 0.7 percent to 31.8 percent of transactions and include errors that result from SMS software issues. When these errors occur, schools must not only resubmit the data for reprocessing, but there may be an increased chance of data being lost.

ADE can improve SMS software by monitoring the performance of the different packages, providing more timely opportunities for vendors to test changes to their packages, and considering rating or certifying software packages.

Recommendations

ADE should:

- Implement additional controls over data processed through SAIS;
- Archive SAIS reports;
- Establish a tactical team to address stakeholders' concerns; and
- Improve oversight of SMS software.

ADE Needs To Improve IT Management and Oversight

ADE has not followed a standard, structured approach for managing the development of IT projects.

Systems development is unstructured—In most cases, ADE's information systems have not been developed by following a standard or structured process. For example, not all changes to applications have gone through a Quality Assurance group. The lack of a standard system development process has resulted in problems in both implementing and maintaining some information systems.

In addition, system developers frequently fail to document how the systems function. Documentation is needed to maintain and modify systems and develop user instruction manuals. Because of the lack of documentation, IT staff may spend excessive time trying to understand how the applications work.

ADE needs an effective development process—ADE should adopt an effective Systems Development Lifecycle (SDLC). SDLCs provide a structured approach to systems development and outline the key steps a system should go through. Following the SDLC will help ensure that systems meet IT objectives, comply with laws and rules, and are adequately documented.

Although ADE's Project Management Office has created a guide to help direct information systems development, it does not include all of the steps found in a good SDLC.

Need to improve oversight of IT operations—ADE should also improve the management of its IT operations and can take three actions to do so:

1. Develop and actively monitor key IT performance indicators, such as system downtime.
2. Regularly perform IT risk assessments, such as loss of key personnel, and address the issues raised from such assessments.
3. Fully develop a business continuity plan.

Recommendations

ADE should:

- Develop, adopt, and enforce an effective systems development process; and
- Establish performance measures, conduct risk assessments, and develop a business continuity plan.

ADE Should Ensure That Its IT Efforts Meet Its Business Needs

ADE needs to improve how it plans and prioritizes the use of its IT resources.

IT not included in strategic planning— Although IT resources may be needed to meet the goals in ADE's strategic plan, the IT section is not effectively included in ADE's strategic planning process. For example, ADE lacks a process for identifying the IT resources needed to achieve ADE's strategic objectives.

No process for prioritizing IT projects— ADE also lacks a department-wide process to prioritize IT projects to ensure agency-wide priorities are met. Instead, the IT section often prioritizes IT projects without input from ADE management or the affected divisions.

ADE should establish steering committee—To ensure adequate IT involvement in strategic planning, and to establish an agency-wide process for prioritizing IT projects, ADE should establish an IT steering committee composed of upper ADE management and the chief information officer.

IT section needs to improve its planning process—The IT section's own planning process is poor. It does not identify the resources it needs to maintain current operations or plan for future IT initiatives. The current plan was developed without any stakeholder input and does not address ADE's strategic objectives. It has also remained virtually unchanged for the past 2 years and has at least four obsolete objectives.

Recommendations

ADE should:

- Establish a steering committee to provide agency-wide IT direction; and
- Ensure that the IT section has an effective planning process.

TO OBTAIN MORE INFORMATION

A copy of the full report can be obtained by calling (602) 553-0333

or by visiting our Web site at: www.azauditor.gov

Contact person for this report: Joseph D. Moore