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.