A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Procedural Review

Arizona State University

As of July 11, 2003

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.

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.auditorgen.state.az.us

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

WILLIAM THOMSON
DEPUTY AUDITOR GENERAL

May 11, 2004

The Arizona Board of Regents
2020 North Central Avenue, Suite 230
Phoenix, AZ 85004

Michael Crow, Ph.D., President
Arizona State University
Box 872203
Tempe, AZ 85287-2203

Dear Dr. Crow:

We have performed a procedural review of Arizona State University (University) internal controls over its information technology systems, including the University's electronic commerce/electronic government-related systems in effect as of July 11, 2003. Our review consisted primarily of inquiries, observations, and selected tests of internal control policies and procedures, accounting records, and related documents. The review was more limited than would be necessary to give an opinion on internal controls. Accordingly, we do not express an opinion on internal controls or ensure that all deficiencies in internal controls are disclosed.

Specifically, we reviewed the Advantage financial system, as well as the tuition payments and student accounts computer systems. This review included application controls relating to accounts receivable, student fees, accounts payable, payroll, and journal entry transaction cycles. This review also included general controls relating to access, program change, backup and recovery, system development and acquisition, computer operations, database, telecommunications, network, and Internet and electronic commerce.

As a result of our review, we noted certain deficiencies in internal controls that the University's management should correct to ensure that it fulfills its responsibility to establish and maintain adequate internal controls. Our recommendations to correct these deficiencies are described in the accompanying summary.

This letter is intended solely for the information and use of the Arizona Board of Regents and the University and is not intended to be and should not be used by anyone other than the specified party. However, this letter is a matter of public record, and its distribution is not limited.

Should you have any questions concerning our procedural review, please let us know.

Sincerely,

Debbie Davenport
Auditor General

TABLE OF CONTENTS

Introduction & Background

The Office of the Auditor General has conducted a procedural review of Arizona State University's e-commerce and information technology systems for fiscal year 2002-2003. The University uses it numerous computer systems for virtually all of its operations, from student to financial services. Of particular importance, the University uses the internet and e-commerce to conduct business. For example, approximately 70% of all student tuition and fee payments are processed using the tuition payments and student account systems.

The University has a fiduciary responsibility to its students, employees, and the general public to safeguard any confidential or sensitive information received by the University. For example, as the University uses the Internet and e-commerce to collect payments from students, it is important that the University safeguard personal student information. Our review evaluated whether the University had established adequate controls and proper monitoring procedures to process and safeguard its sensitive electronic information.

University History & Demographics

Arizona State University (ASU) was originally established in Tempe, Arizona in 1885 by an act of the Thirteenth Territorial Legislature as a teachers college. Today, the University is one of the leading metropolitan research universities in the nation and home to more than 55,000 undergraduate, graduate, and professional students. In addition to the main campus in Tempe, the University is comprised of three other campuses: ASU West, in northwest Phoenix, ASU East, in Mesa, and ASU's extended campus based out of downtown Phoenix.

Funding Sources & Uses

In the fiscal year ended June 30, 2003, the University received $846 million in revenue and had total expenses of $839.1 million. Specific revenue sources and uses were as follows (dollars in millions):

SOURCES	
State appropriations	$311.8
Tuition and fees, net of allowances	206.2
Grants and contracts	158.7
Other sources	169.3
Total Sources	$846.0
USES	
Instruction and academic support	$375.3
Research and public service	122.8
Student services and institutional support	93.5
Other uses	247.5
Total Uses	$839.1

Source: Audited financial statements

Scope and Methodology

As part of our review, we used the National Electronic Commerce Coordinating Council's (NECCC) *Risk Assessment Guidebook For e-Commerce/e-Government* to evaluate the critical functions of the University's computer systems. The areas reviewed were as follows:

- Leadership and Governance—planning, guiding, establishing targets, measuring results, and holding those responsible accountable for meeting goals.
- Privacy—protecting citizens' private information by guarding against disclosure of confidential information.
- Security—protecting data where it is stored and during transmission.
- Technology—controlling the plan, design, development and implementation of computer hardware and software systems.
- Legal Readiness—ensuring an effective legal framework for the electronic government.
- Customer Readiness and Accessibility—addressing the barriers that may limit the intended citizens' use of an e-government system.
- Applications—developing systems to ensure data is gathered and processed correctly.
- Competencies—ensuring the competence of the human resources dedicated to support the e-government effort.

In performing our review, certain information came to our attention that because of its sensitive nature has not been included in this report. However, this information has been provided to University's management for their review and appropriate corrective action.

As a result of our review, we noted the following areas where the University can improve its controls over its information technology systems:

- Software systems changes
- Disaster recovery plan
- Service organization audits
- Removal of confidential data
- Risk assessments
- Access controls

The Auditor General and her staff express appreciation to University personnel for their cooperation and assistance throughout the review.

Recommendations

The University needs policies and procedures for software systems changes

Effective written policies and procedures for program changes, including operating systems and application programs, databases, firewalls, and Web site pages provide the basic framework for establishing employee accountability. They serve as a reference tool for employees to help ensure that requests for changes have been properly authorized and changes are appropriately made and tested before being placed into operation. A well-designed and properly maintained system of policies and procedures enhances both accountability and consistency. Also, written policies and procedures help to explain the design and purpose of control-related procedures, which can increase employee understanding and support for controls. However, the University did not have documented policies and procedures for requesting, reviewing, approving, or testing of changes to its financial, tuition payments and student accounts software systems. Without adequate policies and procedures, the University risks making erroneous or unauthorized changes to programs, databases, firewalls, and Web pages.

Written policies and procedures help ensure system changes are authorized, tested, and understood by employees.

To safeguard its sensitive electronic information, the University should develop and implement written policies and procedures for information system changes, including those relating to e-commerce systems. These policies and procedures should ensure that:

- All changes to information systems are authorized, analyzed, designed, tested, documented, and approved prior to being placed into production.
- Authorization is obtained from user management prior to program changes.
- Management and users review and approve the testing methodology.
- All changes are adequately documented.
- All changes are reviewed, approved, and tested by an independent person.
- Previous versions of information system changes (i.e., version control) are maintained.

The University should have a well-documented, current, and tested disaster recovery plan

Disaster recovery plan had not been updated since 1993.

A properly designed disaster recovery plan helps ensure that proper procedures are in place to provide for the continuity of operations and that electronic files of financial data are not lost in the event of a disaster or other business interruption. However, the University's disaster recovery plan had not been updated since 1993 and had not been tested to determine its effectiveness. Further, the plan did not address any of the University's current e-commerce systems, identify specific threats to the University, or designate an alternate location to process data.

A current, well-developed, and tested disaster recovery plan will help ensure electronic data is properly secured and minimize the length of interrupted computing services. Accordingly, the plan should include:

- Personnel assigned to disaster teams, and operating procedures and emergency telephone numbers to reach them.
- Arrangement for a designated physical facility.
- A risk analysis identifying the critical applications, exposures, and assessment of the impact on the entity.
- Arrangements with vendors to support the needed hardware and software requirements.
- Forms or other controls documents to use in case of a disaster.

Further, the plan should be updated and tested on a regular basis with a copy of the plan stored off-site.

The University should review service organization audit reports

The service organization processed and collected $181 million in student tuition, fees, and other charges during calendar year 2002.

One of the services the University provides its students is for the payment of tuition and fees over the Internet through its Sun Dial interactive voice and Web site system. The University relies on a service organization to process and collect these payments. The service organization had an independent audit performed over its internal controls. Independent audits are a customary way to determine if transactions are being appropriately processed and if data received is being properly safeguarded. Also, the University places complete reliance on the internal controls established by the service organization for processing these transactions. However, the University had not obtained a copy of the internal control report of the service organization to evaluate its operations.

Consequently, the University had no information regarding the outcome of the independent audit or the adequacy of the service organization's security or other information systems controls.

The University should obtain and review the audit reports of any service organization it uses, such as the one processing the University's e-commerce transactions. In addition, during the procurement process, the University should identify the specific security measures that it considers necessary to safeguard its transactions, including privacy and confidentially during transmission and storage of data.

Confidential data should be securely removed from disposed or reused computers

When disposing of or reassigning computer hardware, using certain secure data elimination techniques helps prevent access to confidential information by removing all traces of data previously stored on the equipment. However, the University did not use secure data removal techniques. The disk reformatting or removal utilities that are part of standard computer operating systems are not sufficient to ensure the data cannot be subsequently retrieved. To help ensure that unauthorized access to confidential data does not occur, the University should develop and implement a policy that requires the use of a secure data elimination technique, such as disk scrubbing, when disposing of or reassigning computer equipment.

The University should perform periodic information systems risk assessments

Risks, including unauthorized use and ineffective disaster recovery, are associated with any information system. To understand and manage the risks associated with its information systems, the University should perform periodic risk assessments. The Information Systems Audit and Control Association's Guide, *Control Objectives for Information and Related Technology* (COBIT), provides one example for a framework for management to understand and manage the risks associated with new technologies. The COBIT guidelines emphasize the importance of performing periodic risk assessments to identify and assess security threats and potential vulnerabilities within the system, and to ensure that safeguards are in place for reducing or eliminating the identified risks. However, the University had not performed risk assessments to determine the potential threats to its information systems, including its e-commerce systems.

The University should perform periodic risk assessments of its information systems. For example, the guidance reflected in COBIT could be followed to help identify the security threats and potential vulnerabilities of the University's systems. Once the risk assessment has been completed, the University should establish feasible internal control safeguards for reducing or eliminating the identified risks.

Computer access controls should be strengthened

System access controls help ensure that only authorized users have access to read, create, or modify data in a system. Policies and procedures requiring timely deactivation of users who terminate employment or transfer positions and also requiring passwords be changed periodically, helps reduce the risk of theft, manipulation, or misuse of sensitive information.

The University's system did not automatically deactivate users with administrative access privileges who terminated employment or transferred to another position. Instead, system administrators must manually remove these user accounts. This often results in significant delays in closing accounts, leaving the University's systems at increased risk of unauthorized access. Auditors noted that the network access user name and password (i.e., asurite id) had been cancelled for employees. However, the administrative access for the security system had not been deactivated for 155 former employees. In addition, one of the University's major systems did not automatically prompt employees to change passwords periodically.

The University should improve its policies and procedures over system access to help reduce the risk of theft, manipulation, or misuse of its sensitive information. Specifically, the University should deactivate all access rights immediately after an employee's termination or transfer. In addition, system changes should be made that require user passwords to be changed periodically.

Other Pertinent Information

During our review of the University's information technology system, we noted that the University's accountability for systems policies and procedures were spread among numerous individuals. In addition, the University did not document its security policies and procedures, and there was no evidence that appropriate personnel received periodic updates to security policies.

Based on this information and our review, it appears that the University might benefit from a more accountable approach in coordinating its information technology systems. For example, some organizations have a central IT director or coordinator to oversee organization-wide responsibilities such as ensuring that applicable information system controls are fully documented and appropriately managed, and that adequate security measures are placed into operation.

ARIZONA STATE UNIVERSITY

TEMPE, ARIZONA 85287

October 27, 2003

Debbie Davenport
Auditor General
2910 N. 44th Street, Suite 410
Phoenix AZ 85018

Dear Ms. Davenport

Arizona State University (ASU) presents below, responses relating to your procedural review of the University's internal controls over its information technology systems, primarily the University's electronic commerce/electronic government-related systems. We understand that this was a pilot review with ASU being the first state agency selected.

Recommendation 1: The University needs policies and procedures for software system changes.

We agree that improvement in this area is desirable. We note that many controls are in place, but that the amount of formalization of policies and procedures should be increased.

Recommendation 2: The University should have a well-documented, current, and tested disaster recovery plan.

We Agree. ASU has recently appointed a Business Continuity Officer and we know that disaster recovery planning is part of the scope of this new position. We believe our approach of including disaster recovery planning as a subset of business continuity planning is a significant step forward.

Recommendation 3: The University should review service organizations reports.

We agree. The independent audit report on internal controls for the service organization that the University is migrating towards, has been obtained and reviewed. Future selection processes for service organizations will include the requirement that the independent audit report on internal controls (SAS 70 report) will be obtained and reviewed. In addition, the annual independent audit report on internal controls for the service organization selected will be obtained each year and reviewed for any significant internal control weaknesses identified by the auditors.

ka.42w-410

Recommendation 4: Confidential data should be securely removed from disposed or reused computers.

We agree.

Recommendation 5: The University should perfom periodic information systems risk assessments.

We agree. ASU's central IT organization is looking forward to having a fairly Comprehensive external review in late 2003. We will ask the reviewers to be mindful of risk assessment issues. In addition, a recently created position of (IT Security Liaison) will be charged with periodic risk assessment.

Recommendation 6: Computer access controls should be strengthened.

We agree with the recommendation to strengthen controls. We note that the "chain" of Permissions needed to access systems had indeed been properly broken by automated methods. There was, however, virtually no risk of unauthorized access to systems.

Other Pertinent Information:

We take respectful note of this information and agree with it to a significant extent.

We have appreciated the opportunity to formally respond to the recommendations. If there are any questions or further clarification is desired, please contact either of us.

Sincerely,

William E. Lewis
Chief Information Officer
and Vice Provost

Mernoy E. Harrison, Jr.
Executive Vice President
for Administration and Finance