A REPORT
TO THE
ARIZONA LEGISLATURE

Performance Audit Division

Performance Audit

Arizona's Universities—
Information Technology Security

June • 2008
REPORT NO. 08-04

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 **John Nelson,** Chair

Representative **Tom Boone**
Representative **Jack Brown**
Representative **Pete Rios**
Representative **Steve Yarbrough**
Representative **Jim Weiers** (*ex-officio*)

Senator **Robert Blendu,** Vice Chair

Senator **Carolyn Allen**
Senator **Pamela Gorman**
Senator **Richard Miranda**
Senator **Rebecca Rios**
Senator **Tim Bee** (*ex-officio*)

Audit Staff

Melanie M. Chesney, Director

Dot Reinhard, Manager and Contact Person
Anne Hunter, Team Leader
Travis Alexander
Melinda Gardner
Brian Miele
Dana Payne

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

June 19, 2008

Members of the Arizona Legislature

The Honorable Janet Napolitano, Governor

Dr. Michael M. Crow, President
Arizona State University

Dr. Robert N. Shelton, President
University of Arizona

Dr. John D. Haeger, President
Northern Arizona University

Mr. Joel Sideman, Executive Director
Arizona Board of Regents

Transmitted herewith is a report of the Auditor General, A Performance Audit of Arizona's Universities—Information Technology Security. 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 Arizona Revised Statutes §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 their responses, Arizona State University, the University of Arizona, and Northern Arizona University agree with the findings and plan to implement the recommendations specific to them. In addition, a response from the Arizona Board of Regents is included.

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

This report will be released to the public on June 20, 2008.

Sincerely,

Debbie Davenport
Auditor General

Enclosure

cc: Mr. Fred Boice, President
Arizona Board of Regents

SUMMARY

The Office of the Auditor General has conducted a performance audit of information technology security at Arizona State University (ASU), the University of Arizona (UA), and Northern Arizona University (NAU) 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 performance audits of the universities. The other two audits focus on technology transfer programs and capital project financing.

Information technology (IT) security practices are important for Arizona's universities to protect large amounts of sensitive and confidential information that are stored on their computer systems, including information for more than 122,000 students and nearly 25,000 faculty and staff. Universities in general are attractive targets for computer hackers because universities traditionally have a strong culture of academic freedom that values open access to information and a free exchange of ideas. By providing numerous computers and high-capacity Internet access that allows for a large exchange of information at high speeds, universities not only accommodate their many users, but also create an attractive target for computer hacking. University IT security problems are occurring more often through weaknesses in computer programs called Web-based applications. Web-based applications are popular because users can view or update information over a Web browser, such as Internet Explorer, rather than having to download the programs onto their personal computers. The Arizona universities combined use at least 205 significant Web-based applications for educational and administrative purposes, such as curriculum and course management, documenting personal information for admissions and financial aid, and processing financial, payroll, and other transactions, such as purchasing parking permits.

Universities need to improve Web-based application security (see pages 9 through 15)

ASU’s, UA’s, and NAU's Web-based applications are vulnerable. Auditors were able to gain unauthorized access to sensitive information, such as social security numbers, and could have modified or deleted important university information.

Auditors were able to gain this access by exploiting some critical and commonly found weaknesses that exist in many of the universities' Web-based applications. For example:

- Security weaknesses in one Web-based application allowed auditors to access a database and obtain more than 10,000 records with names and social security numbers. Auditors also obtained other records that contained student identification numbers, addresses, phone numbers, and e-mail addresses. Auditors also had the ability to modify and delete this information.

- In two other applications, auditors were able to exploit a security weakness that would have allowed them to take over a large number of user accounts, including accounts with high-level access.

- In many applications, auditors discovered a security flaw that would allow an attacker to take over user accounts and install malicious software.

Such vulnerabilities are likely to exist in many more of the universities' Web-based applications. Auditors did not attempt to identify every flaw that may exist because the testing was designed to determine what the impact could be if certain identified vulnerabilities were successfully exploited. However, based on the results, auditors concluded that the security flaws they identified are likely to exist in other university Web-based applications.

To better protect the information processed through their Web-based applications, ASU, UA, and NAU need to:

- Conduct regular security assessments of Web-based applications. The universities first need to determine how many Web-based applications they have and then make provisions to regularly update their lists of applications. They then need to develop and implement procedures for regularly conducting security reviews of their critical Web-based applications.

- Develop a university-wide policy and associated procedures for updating Web servers, which are computers that host Web-based applications. Software vulnerabilities are constantly being discovered and publicized, and the universities need to develop or enhance: (1) procedures for identifying vulnerabilities relevant to their Web servers, (2) a timeline for reacting to notifications of newly discovered Web server vulnerabilities, and (3) a process for determining whether to apply a software update, establish another control to address the Web server vulnerability, or accept the risk of not updating the software.

- Ensure that security is built into the process for developing Web-based applications. According to ASU, UA, and NAU officials, none of them have

[1] Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007.

university-wide security standards for developing applications. According to an IT best practice, building security into the development process is more cost-effective and secure than applying it afterwards.[1]

- Provide training to application developers so that they are aware of common Web-based application vulnerabilities and methodologies that can be used to avoid them. None of the universities have a training program that is mandatory for all users and geared toward an individual's role within the university.

Universities need to develop comprehensive IT security programs (see pages 17 through 28)

All three Arizona universities have taken some key steps toward developing an overall IT security approach; however, additional work is needed.

- **Creating information security staffs**—Over the past few years, ASU, UA, and NAU have established and filled information security officer (ISO) positions and made these ISOs responsible for information security efforts university-wide. Until the ISOs were hired, the universities have not had any staff whose sole responsibility included directing and coordinating all aspects of information security across the university.

- **Developing information security programs**—The universities are at varying stages in developing formal programs to guide their information security efforts, but none have yet developed all the standards or procedures needed to support a complete information security program. The universities are in the beginning stages of implementing their information security programs, in part because the ISO positions are relatively new. All three universities' programs will consist of an overall information security policy and supplemental standards that will provide guidance on how to implement key information security features. According to IT standards and best practices, an effective information security program consists of at least four key security features: (1) classifying and protecting data according to its sensitivity, (2) conducting risk assessments, (3) providing users with security awareness education and training, and (4) responding to information security threats or incidents. The universities' programs lack many of the policies, standards, or procedures needed to effectively address these features.

  ASU, UA, and NAU also need to identify the necessary resources for implementing their information security programs, including determining whether they have adequate resources internally or need to request additional funding. Then, after their programs are put in place, the universities need to monitor university-wide program compliance.

TABLE OF CONTENTS

INTRODUCTION & BACKGROUND

The Office of the Auditor General has conducted a performance audit of information technology security at Arizona State University (ASU), the University of Arizona (UA), and Northern Arizona University (NAU) 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 performance audits of the universities. The other two audits focus on technology transfer programs and capital project financing.

Information technology security important for universities

Information technology security protects sensitive information and ensures authorized users can access information.

Information technology (IT) security practices are important for Arizona's universities to protect large amounts of sensitive information stored on their computer systems. IT security primarily involves the protection of electronic information from unauthorized use and the ability to deliver complete and accurate data to authorized users. For example, IT security practices can help prevent unauthorized individuals from accessing, modifying, or deleting confidential information from computers, and can also prevent them from causing computer systems to malfunction and denying access to legitimate users. Arizona's universities—ASU, UA, and NAU—are responsible for many diverse and complex computer systems that provide student services and academic and administrative support. These computer systems process various types of information such as contact information, social security numbers, and credit card numbers for nearly 25,000 faculty and staff, more than 122,000 students, some of the 625,000 alumni, and others, including prospective students applying for admission.[1]

IT security is becoming increasingly important to protect individuals' and universities' information and computers from unauthorized use or access. According to an October 2006 study by the Educause Center for Applied Research (ECAR), 26 percent of the 492 universities surveyed reported that confidential information had been compromised in identified IT security incidents.[2] In addition, 29 percent of the

[1] Faculty and staff totals, not including student employees, and the unduplicated student total were obtained from the Arizona Board of Regents, and alumni totals were compiled from each university's alumni association Web site.

[2] Caruso, Judith Borreson. "ECAR Key Findings-Safeguarding the Tower: IT Security in Higher Education 2006." October 2006. Educause Center for Applied Research. August 24, 2007 <http://www.educause.edu/ir/library/pdf/EKF/Ekf0606.pdf>. Established in 2001, ECAR is the research organization within Educause, which is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

IT security is needed to protect universities from increased computer security violations.

universities reported computer network unavailability and 34 percent reported e-mail unavailability as a result of IT security incidents. The study also stated that IT security threats are continually increasing and becoming more harmful and complex, requiring additional protective measures. Similarly, an October 2006 study funded by the U.S. Department of Justice found that two universities detected almost 2 million attempted security violations in 4 months.[1] The same study reported that of the 72 universities surveyed, 47 percent detected an increase in attempted security violations from the previous year.

IT security violations have occurred both in Arizona and other states. For example:

- The University of Arizona discovered in February 2006 and January 2007 that attackers traced to foreign countries had unauthorized access into the university's computer systems. Although UA found no evidence of data theft, the 2006 break-in disrupted the journalism department, and the 2007 break-in disrupted a procurement system, university library services, and a payroll processing and meal plan system. Some services were shut down for several days to restore affected computer systems.

- Ohio University was informed in April 2006 about one of a series of computer systems breaches that resulted in 137,000 compromised social security numbers and 367,000 files containing personal information that had been exposed for up to 13 months. In addition, medical records for thousands of current and former students, professors, and staff were exposed for 5 months. In response, Ohio University spent $77,000 notifying alumni and students of the security breaches, and $750,000 in emergency-response expenses for computer hardware and consulting; and was allotted $4 million by the Board of Trustees to secure its IT systems. In addition, a class action lawsuit alleging violation of privacy was filed against the university.

IT security is also essential to help universities comply with federal laws and regulations designed to protect sensitive information such as educational records, personally identifiable information, financial aid records, and health information.[2] Arizona laws also require some elements of IT security. A.R.S. §44-7501, for example, requires any person or entity in Arizona holding computerized records to notify individuals about compromised personal information if the compromise places these individuals at risk of substantial economic loss.

[1] Burd, Steffani A. "The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice." Report submitted to the U.S. Department of Justice, Grant No. 2004-IJ-CX-0045. October 2006. U.S. National Criminal Justice Reference Service. September 6, 2007 <www.ncjrs.gov/pdffiles1/nij/grants/215953.pdf>.

[2] Some pertinent laws and regulations include the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g and 34 C.F.R. §99; the Gramm-Leach Bliley Act (GLBA), 15 U.S.C. §§6801-6809 and 16 C.F.R. §314; and the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191 and 45 C.F.R. §§160-164.

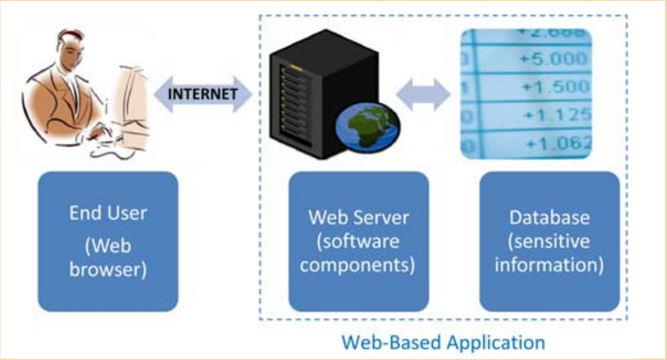
IT security challenges at universities

Many universities have begun to address these computer security issues in greater depth, though they face a number of challenges in doing so. Because of their tradition of open access to information, as well as their numerous computer users, universities have typically been targeted by computer hackers—those who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Protecting systems is made more difficult by the extensive use of computer programs called Web-based applications, which offer convenience for university staff and students but also cause increasing IT security problems. Typical steps that universities have begun to take include adding staff positions focused on information security and developing information security programs.

Universities are attractive targets for computer hackers.

IT security challenging at universities—University environments are not always conducive to IT security. In general, universities traditionally have a strong culture of academic freedom that values open access to information and a free exchange of ideas. By providing numerous computers and high-capacity Internet access that allows a large exchange of information at high speeds, universities not only accommodate their many users, but also create an attractive target for computer hacking. Computer hackers may also be attracted to universities because the high turnover in computer users results in a constant supply of new information to exploit. In addition, universities typically develop IT processes and store data at the department level more than at the central level. Although this type of organizational structure may be more convenient and customized for the departments, the studies cited earlier indicate that providing adequate university-wide IT security in this type of structure can be difficult.

Web-based applications an increasing risk to IT security—IT security problems are occurring more often through weaknesses in computer programs called Web-based applications, which allow users to access programs through their Internet browser rather than requiring users to download the programs onto their personal computers (see textbox). The universities and many of their departments provide IT services in this manner. For example, ASU provides a Web-based application to students and employees to manage campus parking. Individuals can go to the designated Web site on the Internet to purchase parking



A **Web-based application** is a software program or system that is accessed by an **end user** to perform a transaction with a Web browser, such as Internet Explorer, over a network such as the Internet. Software components usually reside on a **Web server**, which is a computer that retrieves information, usually from a **database**, and sends it to the **end user's** Web browser for display. This process provides the ability to update and maintain Web-based applications without the need to distribute and install software on end-user computers, which is a key reason for their popularity.

Source: Auditor General staff analysis of IT definitions from various sources.

permits and pay and appeal citations. The Web-based application software components and data are stored on computers at ASU, and information is exchanged with the individuals' computers by a Web server.

Sensitive information can be taken from poorly developed Web-based applications.

Web-based applications, although convenient for users, can introduce security risks if not developed properly or if associated software is not adequately updated. For example, if the developers did not build in preventive security measures, someone with access to the Internet could exploit a Web-based application weakness and gain access to sensitive information stored by the Web-based application, such as social security numbers or credit card numbers. The State's three universities combined have at least 205 significant Web-based applications used for educational and administrative purposes such as curriculum and course management, documenting personal information for admissions and financial aid, and processing financial and payroll transactions.

Many universities are beginning to use information security programs and information security officers.

Universities have started addressing IT security challenges—According to the October 2006 ECAR study, higher-education institutions have taken significant steps to improve their IT security, but still have room for improvement.[1] According to the study, steps taken by some universities include adopting an information security program and hiring an information security officer. An information security program should be a formalized agency-wide written plan that specifies how IT security will be administered through key features, such as security awareness training and assessing the risks of information security violations. Information security officers should be responsible for organization-wide IT security and for implementing the information security program. According to the ECAR study, 35 percent of the 492 universities responding had an information security officer, and 11 percent reported that they had an information security program in place. The ECAR study indicates that universities need to continue efforts such as adopting an information security program in order to ensure that IT services are secure and data is protected.

Universities' IT staff, expenses, and organization

In fiscal year 2007, ASU, UA, and NAU used more than 2,300 full-time equivalent (FTE) positions and $229 million for IT-related purposes university-wide. According to university reports, IT-related FTE employees and expenses included ASU's 1,283 FTEs and more than $106 million; UA's 784 FTEs and more than $91 million; and NAU's 253 FTEs and more than $32 million.[2] IT staff indicated that IT functions include purchasing, maintaining, and repairing computers; setting up and troubleshooting computers used by faculty, staff, and students; and supporting users in computer labs. They also stated that IT expenses are incurred for things such as hardware, including mainframes, servers, and personal computers; peripheral devices such as printers and scanners; supplies such as printer cartridges and

[1] See footnote 2, page 1.

[2] FTE and expenses information compiled from the universities' fiscal year 2007 IT annual reports dated October 10, 2007, and submitted to the Arizona Board of Regents.

paper; software programs; networking capabilities, including phone and Internet services; maintenance contracts on software and equipment; and IT staff salaries. Although the universities do not track university-wide IT security expenses, the central IT offices at ASU, UA, and NAU estimated using at least 1.0, 2.8, and 1.0 percent, respectively, of their fiscal year 2007 budgets on IT security. The October 2006 ECAR study reported that among the 492 universities responding, the universities' central IT offices spent, on average, between 1 and 5 percent of their budgets on IT security.

Arizona's universities do not track university-wide IT security expenses.

Each of Arizona's three universities has a central IT office with an IT staff that is responsible for services that benefit the entire university. A Chief Information Officer (CIO) is in charge of IT for the entire university. An information security officer (ISO) reports to the CIO and takes responsibility for university-wide IT security. Other staff spend a portion of their time working on IT security issues, but as of March 2008, only one or two staff members in each office, including the ISO, were solely dedicated to information security (see Finding 2, page 17). Central staffing for IT security at many universities has grown, according to the ECAR study. For example, the proportion of the 204 respondents with more than 5 central staff members dedicated to IT security doubled between 2003 and 2005.

Universities receive IT security oversight and assistance from Board of Regents

Since 2002, the Arizona Board of Regents (Board) has taken several steps to oversee and assist with the universities' IT security issues. The Arizona Constitution and state law authorizes the Board to govern and set regulations for the universities and to adopt their budgets.[1] In 2001, the Office of the Auditor General reported that the Board could improve oversight of university information technology projects and recommended that the Board implement an oversight process for IT projects that includes a review of the justification for such projects (Report 01-27). In response, the Board formed the Technology Oversight Committee (Committee) in 2002.[2] By the following year, the Board, through the Committee, began to review the universities' annual IT Implementation Plans, which include IT project justifications, IT accomplishments, IT expenses, and IT FTEs. These plans also include information relevant to IT security. In 2004, the Board approved a “Tri-University IT Architecture” document, which contains general IT principles, standards, and best practices in six areas, including IT security.

In recent years, the Board has taken an increased role with regard to IT security. The Board paid for two assessments—in 2003 and 2005—of the three universities' security over their computer networks. In 2005, the Board requested an analysis of how well the universities were complying with the Tri-University IT Architecture. In 2006 and 2007, it also requested that the universities conduct and submit additional assessments on the status of their IT security. In 2006 and 2007, the Board's internal

[1] Arizona Constitution, Article XI, §2 and §5; A.R.S. §§15-1625 through 15-1626.

[2] In 2002, the Committee was called the Arizona Regents Information Technology Team and in 2007 was renamed the ABOR (Arizona Board of Regents) Technology Oversight Committee.

audit staff studied issues related to IT security in computer systems located outside the central IT office for each university. Although most of these studies indicated that some appropriate IT security practices were in place, specific Web-based applications were not tested for security vulnerabilities. In addition, the assessments showed that areas such as creating policies and preventing unauthorized access needed improvement. The Committee, a board staff member, and the universities' CIOs periodically meet to discuss progress on areas needing improvement. They have also worked with a consultant and university IT staff to develop policies, guidelines, and standards related to IT security. In addition, the Committee hired another consultant to identify ways for the universities to collaborate on their IT efforts. The consultant's report, released in 2007, recommended that the universities work together to conduct regular vulnerability scans and that the Committee's focus should be on the oversight and policy implications of major IT initiatives.

Scope and methodology

This audit focused on IT security at ASU, UA, and NAU and covered three areas: Web-based application security, information security officers, and information security programs. This report presents two findings and associated recommendations, as follows:

- **Universities need to improve the security of their Web-based applications**—Auditors were able to obtain access to sensitive information, such as social security numbers and contact information, as well as gain access that could have allowed them to modify or delete sensitive university information by exploiting weaknesses in several university-developed Web-based applications. To address these security weaknesses, the universities need to develop plans for regularly assessing and correcting Web-based application vulnerabilities, updating the software on their IT systems, and establishing and following security standards for developing Web-based applications, including providing security awareness training to application developers. They should also work with the Board to establish timelines for implementing the audit recommendations and regularly report on the progress of their implementation efforts.

- **Universities need to develop comprehensive IT security programs**—ASU, UA, and NAU have taken a key step toward helping to ensure that sensitive information and systems are adequately protected by establishing and filling ISO positions. In line with IT standards and best practices, these ISOs have been tasked with establishing university-wide information security programs. However, because these ISOs are relatively new to their positions, the universities are in the early stages of developing these programs. As they proceed with implementation, the universities will need to ensure that they establish formalized processes in line with IT standards and best practices, and include key security program features such as security awareness education and training and incident response. In addition, the universities will need to enhance their IT security planning and monitoring efforts by identifying the resources needed to implement their information security programs and continuing with their plans for monitoring compliance with the security program. Further, they should work with the Board to establish timelines for implementing the audit recommendations and regularly report on the progress of their implementation efforts.

Auditors used several methods to study the issues addressed in this audit. Methods used in all areas included reviewing IT standards and best practice guides, and ASU, UA, NAU, and the Board's policies.[1] Auditors also interviewed university management and staff and the Board's executive management and staff. In addition, the following methods were used in reviewing each specific area:

- To evaluate the security of university Web-based applications, auditors and an independent security consultant retained by the Office of the Auditor General tested Web-based applications and Web servers using both automated and more detailed security testing techniques. To identify the number and nature of the universities' Web-based applications, auditors interviewed university staff, reviewed university documents, and performed technical scanning techniques. Auditors identified at least 205 significant Web-based applications. Using a risk-based approach, auditors then selected 35 of these Web-based applications and 42 associated Web servers to test with automated security scans. These scans identified potential vulnerabilities in the Web-based applications and associated Web servers. Based on the scan results, auditors selected six Web-based applications for further detailed testing. This testing allowed auditors to identify the potential impact of these applications being compromised because of their vulnerabilities. During detailed testing, auditors identified serious vulnerabilities, interviewed staff, and reviewed some university documents to determine the vulnerabilities' causes. Auditors and the consultant then developed specific recommendations on how the vulnerabilities could be fixed. Because of the information's sensitive nature, specific information about the security weaknesses identified has been excluded from this report and shared

[1] IT standards and best practice material reviewed included: (1) *COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models.* Rolling Meadows, IL: IT Governance Institute, 2007; (2) Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007 <http://www.isfsecuritystandard.com>; (3) International Organization for Standardization. *ISO/IEC 27002:2005, Information Technology: Security Techniques: Code of Practice for Information Security Management*. Geneva, Switzerland: International Organization for Standardization, 2005; (4) Meucci, Matteo, and Eoin Keary, eds. "OWASP Testing Guide, 2007 V2." 2007. OWASP Foundation. January 16, 2008 <http://www.owasp.org>; (5) Ross, Ron, et al. *Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53 Revision 2*. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, December 2007; (6) Wiesmann, Adrian, and Andrew van der Stock, eds. "A Guide to Building Secure Web Applications and Web Services, 2.1 Draft 3." February 2006. OWASP Foundation. January 16, 2008 <http://www.owasp.org>; and (7) Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology System: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30*. Gaithersburg, MD: U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, July 2002.

only with appropriate university officials. Finally, once university officials reported to auditors that actions were taken to fix the vulnerabilities identified in the six Web-based applications selected for detailed testing, auditors conducted some limited testing to verify the reported actions.

- To determine if ASU, UA, and NAU each had an individual responsible for IT security with appropriate authority and if the universities had an adequate information security program, auditors analyzed their IT security policies and plans and compared them to IT standards and best practices. Specifically, auditors reviewed the universities' IT security policies, standards, and other documents related to IT security. To identify current and planned IT personnel responsibilities, auditors reviewed policies, job descriptions, university organizational charts, and other supporting documentation. Auditors also attended a meeting held by the Board's Technology Oversight Committee and another meeting about IT security held by UA.

- To develop the Introduction and Background section, auditors compiled information from IT literature, federal and state laws, the Board, and the universities such as computer system assessments, unaudited expense reports, and staffing information, and conducted interviews with university and board staff.

This audit was conducted in accordance with government auditing standards.

The Auditor General and staff express their appreciation to the Arizona Board of Regents and its staff, and the universities' presidents and their staff, for their cooperation and assistance throughout the audit.

FINDING 1

Universities need to improve Web-based application security

Arizona State University (ASU), the University of Arizona (UA), and Northern Arizona University (NAU) need to take steps to ensure that their Web-based applications and the underlying data are secure. The applications auditors tested contained commonly found critical security weaknesses that allow unauthorized access to obtain sensitive information, such as social security numbers, or to perform significant tasks, such as changing student and employee records. To better protect the information processed through their Web-based applications, the universities need to regularly identify and correct Web-based application flaws, properly update and maintain essential software on their information technology (IT) systems, establish security standards for developing and securing Web-based applications, and train their Web developers so that they are aware of common vulnerabilities and how they can be avoided.

Sensitive information and systems exposed because of Web-based application weaknesses

Auditors were able to access sensitive information by exploiting security weaknesses or vulnerabilities in several university-developed Web-based applications.[1] The universities use hundreds of Web-based applications to provide services to various individuals, including students and the public. Auditors identified a number of critical security vulnerabilities in the applications they tested. These weaknesses can be exploited to obtain sensitive information or to compromise internal systems maintained by the universities. Such problems are likely to exist across many of the universities' other Web-based applications as well.

Universities extensively use Web-based applications—ASU, UA, and NAU make extensive use of Internet-accessible Web-based applications for use by

[1] Given the sensitive nature of this information, specific information about these weaknesses has been excluded from the report and shared only with appropriate university officials.

students, faculty, staff, and the public. Although the universities could not provide auditors with a comprehensive list of applications, auditors were able to identify at least 205 significant Web-based applications by reviewing various lists, interviewing university staff, and conducting electronic scans of university systems. Of the 205 significant applications, 71 were at ASU, 97 at UA, and 37 at NAU. These Web-based applications provide many university-related services (see textbox) and are used for various purposes, such as processing employment information, registering students for classes, applying for admissions, purchasing parking permits, and paying parking fines. The type of data processed through these Web-based applications often includes sensitive information such as student records, social security numbers, and credit card numbers (see textbox).

University Services Provided and Data Processed through Web-Based Applications

Types of Services Provided:

- Human Resource & Payroll Administration
- Student Administration & Advising
- Financial/Accounting
- Admissions
- Online Courses
- Parking Services
- On-campus Housing
- Ticket Sales

Types of Data Processed:

- Student Records
- Social Security Numbers
- Driver's License Numbers
- Credit Card Numbers
- Financial Aid Information

Source: Auditor General staff analysis of university-provided Web application information.

Auditors able to access sensitive information—Auditors were able to obtain sensitive information and could have gained unauthorized access to some key internal systems by exploiting commonly found weaknesses in several university-developed Web-based applications. Using a risk-based approach, which included accounting for the extent of use and the sensitivity of the information that could be accessed to determine which systems to review, auditors conducted initial automated testing on 35 of the 205 significant Web-based applications. All of the 35 applications contained commonly found security weaknesses. Auditors then selected 6 applications, again based on risk, for further detailed testing. The purpose of the detailed testing was to determine what the impact could be if unauthorized individuals were able to use these weaknesses to compromise the universities' Web-based applications.

All six of the applications selected for detailed testing contained critical flaws. For example, an unauthorized user could:

Auditors obtained more than 10,000 records that contained names and social security numbers.

- **Obtain personal information**—In one application, auditors were able to obtain and download sensitive information contained in one database used by the application. Using this access, auditors obtained more than 10,000 records that contained names and social security numbers. Auditors also obtained other records containing student identification numbers, employee identification numbers, addresses, phone numbers, and e-mail addresses. These flaws could also be used to modify and delete data in the database.

- **Manipulate records**—In two other applications, auditors found that they could exploit a security weakness that would have allowed them to take over a large number of user accounts, including accounts with high-level access. These weaknesses could be used to view and change sensitive student and employee information.

- **Attack and affect users' computers**—In several of the six applications, auditors discovered flaws that could allow unauthorized individuals to attack other users' computers. Attackers often use these types of flaws to take over user accounts and install malicious software.

Problems likely to exist in many other Web-based applications—Although only six applications were tested in detail, it is likely that critical vulnerabilities exist in many more of the universities' Web-based applications. Auditors did not attempt to identify every flaw that may exist because the testing was designed to determine what the impact could be if certain identified vulnerabilities were successfully exploited. Based on these results, auditors concluded that the security flaws they identified are likely to exist in other university Web-based applications.

Critical vulnerabilities are likely to exist in many of the universities' Web-based applications.

Universities need to take steps to address Web-based application security weaknesses

The security vulnerabilities exist because the universities have not conducted Web-based application assessments, properly maintained Web server software, implemented secure Web development standards, or properly trained application developers. In response to this audit's results, the universities have taken some actions to address the weaknesses found in the Web-based applications, including remediating some of the critical vulnerabilities auditors identified, and according to ASU, UA, and NAU officials, they are developing plans for performing security assessments.

Regular security assessments of Web-based applications needed—This audit was the first security review performed of university Web-based applications; none of the universities conduct regular Web-based application security assessments. IT best practices recommend that critical applications be subject to thorough, independent, and regular security audits or reviews to ensure that proper security has been effectively implemented.[1] Therefore, ASU, UA, and NAU need to develop and implement a plan for regularly assessing their critical Web-based applications that includes:

- Creating and regularly updating an inventory of their Web-based applications and determining the criticality of each application and the data processed.

- Developing and implementing procedures for regularly conducting security reviews that assess whether security requirements and controls are functioning effectively.

- Remediating, based on risk, the problems identified during security reviews.

[1] Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007 <http://www.isfsecuritystandard.com>.

Web server—A computer that hosts a Web site or Web-based application. 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. A single Web server can host multiple Web-based applications.

Source: Auditor General staff analysis of IT definitions from various sources.

Thirty of the 42 Web servers contained potential vulnerabilities because of outdated software or insecure settings.

Processes needed for securely maintaining Web servers—ASU, UA, and NAU need to develop a university-wide policy and associated procedures for updating and maintaining their Web servers (see textbox). Although UA has developed some standards for Web servers, its standards are not finalized and are missing important aspects identified in IT standards and best practices, such as methods for identifying vulnerabilities. Similarly, according to ASU and NAU officials, neither university has comprehensive policies and procedures for properly updating and maintaining their Web servers. Of the 205 significant applications identified, auditors tested 42 of the associated Web servers using an automated security scanning tool. Thirty Web servers contained potential vulnerabilities because of outdated software or insecure settings. IT best practices recommend that organizations should develop a process for reducing the risks resulting from widely known and published Web server vulnerabilities or insecure settings.[1] For example, widely used software companies, such as Microsoft and Oracle, publish information on security vulnerabilities that have been discovered in their software. Therefore, UA should enhance its standards to be in line with IT best practices, and ASU and NAU should establish standards or procedures for updating and maintaining their Web servers. The standards or procedures for each university should include:

- A method for identifying relevant widely known Web server vulnerabilities.
- A timeline for reacting to notifications of newly discovered Web server vulnerabilities.
- A process for determining whether to apply a software update, establish another control to address the Web server vulnerability, or accept the risk of not updating the software.

Security needs to be an integral part of the application development process—To help better ensure the security of Web-based applications, ASU, UA, and NAU need to establish university-wide security standards for developing and securing Web-based applications that are in line with IT standards and best practices. Even though the universities develop new Web-based applications, according to ASU, UA, and NAU officials, none of them have university-wide security standards for doing so. As a result, it appears that the universities' Web-based applications are developed using informal processes or individual departments' own internal processes. Therefore, the universities cannot ensure that security requirements will be uniformly and consistently applied.

It also appears that the universities' Web-based application development processes do not include comprehensive security testing requirements or processes. For example, auditors interviewed eight staff across the three

[1] (1) International Organization for Standardization. *ISO/IEC 27002:2005, Information Technology: Security Techniques: Code of Practice for Information Security Management*. Geneva, Switzerland: International Organization for Standardization, 2005; and, (2) Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007<http://www.isfsecuritystandard.com>.

universities involved in the Web-based application development process and found that although half of them had performed some type of security-specific testing on their Web-based applications, the testing was ad-hoc and not comprehensive.

According to an IT best practice, building security into the development process is more cost-effective and secure than applying it afterwards.[1] IT standards and best practices recommend that organizations employ security practices for development that include information security requirements during all phases, including the definition of requirements, design and construction of the application, testing, and implementation. The security practices should include the following:

- **Gathering security requirements**—Security requirements should include classifying the information according to confidentiality, and detailing how the application will comply with all relevant laws, regulations, and standards.
- **A set of up-to-date secure coding standards or conventions**—These are rules for the development of an application based on best practices.
- **Threat modeling during development**—Threat modeling involves learning how the application works, exploring potential vulnerabilities and threats by thinking of possible ways an attacker would attack the application, and then developing mitigating controls for each of the realistic threats identified.
- **Security testing before releasing a Web-based application to the live environment**—Security testing helps ensure that the Web-based application functions as intended and does not contain critical flaws when it is released.[2]

More security training needed for Web-application developers—

Another important aspect for ensuring security of Web-based applications is to provide training to application developers so that they are aware of common Web-based application vulnerabilities and methodologies that can be used to avoid them. According to ASU, UA, and NAU officials and some IT staff, some university application developers have received limited security training. However, none of the universities have a training program that is mandatory for all users and geared toward an individual's role within the university. Training application developers on security requirements helps teach them how to apply information security controls during the development process.[3] As part of a wider security awareness education and training effort (see Finding 2, pages 17 through 28), ASU, UA, and NAU should provide guidance and training on secure Web-based application development practices to their Web developers.

[1] Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007 <http://www.isfsecuritystandard.com>.

[2] (1) Van der Stock, Andrew, and Adrian Wiesmann, eds. "A Guide to Building Secure Web Applications and Web Services, 2.1 Draft 3." February 2006. OWASP Foundation. January 16, 2008 <http://www.owasp.org>; (2) Meucci, Matteo, and Eoin Keary, eds. "OWASP Testing Guide, 2007 V2.0. OWASP Foundation. January 16, 2008 <http://www.owasp.org>; (3) Information Security Forum.

[3] Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007 <http://www.isfsecuritystandard.com>.

Universities should work with the Board—Because the Arizona Board of Regents (Board) oversees and assists the universities with IT security issues, ASU, UA, and NAU should work with the Board's Technology Oversight Committee to establish timelines for implementing the audit recommendations. The universities should also regularly report to the Committee on the progress of their implementation efforts.

Recommendations:

1. ASU, UA, and NAU should:

   a) Develop and implement a plan for conducting regular security assessments of their Web-based applications. This plan should include:

   - Creating and regularly updating an inventory of Web-based applications and determining the criticality of the applications and the data processed.
   - Developing and implementing procedures for regularly conducting security reviews that assess whether security requirements and controls are functioning effectively.
   - Remediating, based on risk, the problems identified during these security reviews.

   b) Enhance or develop and implement university-wide standards or procedures for updating and maintaining their Web servers. The standards or procedures should include:

   - Developing a method for identifying relevant, widely known Web server vulnerabilities.
   - Creating a timeline for reacting to notifications of newly discovered Web server vulnerabilities.
   - Developing a process for determining whether to apply a software update, establish another control to address the Web server vulnerability, or accept the risk of not updating the software.

   c) Establish and implement a set of university-wide standards for developing secure Web-based applications. These standards should encompass all phases of development and include:

   - Gathering security requirements.
   - Developing a set of up-to-date secure coding standards or conventions.

- Using threat modeling exercises during development.
- Performing security testing before releasing an application to the live environment.

d) Provide guidance and training to Web developers on secure Web-based development practices as part of a wider security awareness education and training effort.

e) Work with the Board's Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

FINDING 2

Universities need to develop comprehensive IT security programs

Although the universities have taken steps to address information technology (IT) security from a university-wide perspective, additional action is needed to ensure that information and systems are adequately protected. Arizona State University (ASU), the University of Arizona (UA), and Northern Arizona University (NAU) have all hired an information security officer (ISO) and have begun to assemble an IT security staff whose responsibilities include directing and coordinating information security efforts university-wide. However, each university needs to ensure that its ISO's authority is communicated and recognized university-wide. All three universities have also begun developing an information security program, but these programs are not yet complete. The universities need to ensure that their programs sufficiently address key features that are critical for identifying information security and privacy risks, and ensuring compliance with legal, regulatory, and contractual requirements. Further, the universities need to identify resource requirements needed to implement their programs and also ensure that program compliance is monitored.

Information security officers hired to address security issues university-wide

ASU, UA, and NAU have taken a key step toward helping ensure sensitive information and systems are adequately protected. By late 2007, all three Arizona universities had created and filled ISO positions and made their ISO responsible for directing and coordinating information security efforts university-wide, including establishing university-wide information security programs (see textbox). As defined, these positions appear to be in line with IT standards and best practices that indicate there should be an individual who has sufficient authority

University Information Security Officer Positions

University	Position Title	Date Filled
ASU	Information Security Officer (ISO)	October 2007
UA	University Information Security Officer (UISO)	September 2007
NAU	Director of Information Security (IS)	January 2005

Source: Auditor General staff analysis of university-reported information.

over information security efforts organization-wide and is responsible for implementing the key features of the information security program.[1]

University Information Security Staff

University	Number of Staff	Position Titles
ASU	1	Information Security Officer
UA	2	University Information Security Officer
		Information Security Coordinator
NAU	2	Director of Information Security
		Information Security Analyst

Source: Auditor General staff analysis of university-reported information.

ASU, UA, and NAU are in the early stages of establishing university-wide, dedicated staff positions for information security (see textbox). According to officials at ASU, UA, and NAU, until adding and filling their respective ISO positions, they have not had any staff whose sole responsibility is to direct and coordinate all aspects of information security across the university. For example, the universities had IT staff who spent time working on some elements of information security or a portion of their time working on information security issues, such as maintaining firewalls to protect university networks. In addition, UA has an Information Security Coordinator who is responsible for some aspects of information security, such as information security awareness education and training, but is not responsible for all elements of information security.[2] Similarly, in January 2008, NAU reported hiring an Information Security Analyst who is responsible for assisting in the development and implementation of information security solutions and providing training on technical security topics.

Although the universities' ISOs appear to have been given the appropriate authority over information security efforts university-wide, additional efforts may be needed to communicate this authority because the ISOs are new to their positions. Specifically:

- At UA, based on discussions with UA officials, auditors identified some concerns regarding whether the ISO's authority is understood or recognized university-wide. For example, it appears that some departments may be resistant to direction from the ISO. However, UA is taking steps to ensure that the ISO's authority is properly understood and recognized, including establishing information security liaisons within various departments who will act as the point of contact between the ISO and the departments regarding information security. UA officials also indicated that they anticipate that as the information security program is implemented over time, the ISO's authority will become more apparent. UA should continue with these efforts to help ensure that its ISO's authority is understood and recognized university-wide.

[1] IT standards and best practice materials used: (1) International Organization for Standardization. *ISO/IEC 27002:2005, Information Technology: Security Techniques: Code of Practice for Information Security Management*. Geneva, Switzerland: International Organization for Standardization, 2005; (2) Ross, Ron, et al. *Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53 Revision 2*. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, December 2007; (3) Information Security Forum. "The Standard of Good Practice for Information Security." 2007. Information Security Forum. November 6, 2007 <http://www.isfsecuritystandard.com>; and (4) Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology System: Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30*. Gaithersburg, MD: U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, July 2002.

[2] From October 2006 until September 2007 when UA hired a full-time information security officer, UA's security coordinator assumed some additional responsibilities in the areas of information security. However, during that time, the coordinator was not responsible for all aspects of information security across the university.

- At ASU and NAU, similar concerns were not identified. However, because the ISOs are just beginning to establish university-wide security programs, ASU and NAU should also seek opportunities to ensure that their ISOs' authority and responsibilities are communicated and understood university-wide.

Universities just beginning to develop information security programs

Because all three universities' ISOs are relatively new to their position, all three universities are in the early stages of developing and implementing their information security programs. Much of the work to date is in accordance with IT standards and best practices, but a considerable amount of development remains to be done.

Effective programs should be formalized and include key features—IT standards and best practices indicate that to provide management direction and support for information security, the information security program should be formalized into an agency-wide written plan that identifies a governance structure such as the method by which information security will be directed, administered, or controlled, and that the plan should be disseminated and communicated to affected persons.[1] In addition, an effective information security program should consist of key features that are critical for identifying information security and privacy risks, and ensuring compliance with legal, regulatory, and contractual requirements (see textbox).

Key Features of an Information Security Program

- **Data classification**—The process of labeling information to show its level of sensitivity or the degree of protection needed when handling the information.
- **Risk assessment**—The process of identifying risks such as threats and vulnerabilities, determining the probability of occurrence, the resulting impact, and the additional security controls that would lessen this impact.
- **Security awareness education and training**—Actions taken to regularly inform and train students, faculty, and staff about information security risks and their responsibility to comply with policies to reduce these risks.
- **Incident response**—Procedures for detecting, reporting, and responding to information security incidents, such as a breach of confidential information due to a failure of IT security safeguards or computer hacking.

Source: Auditor General staff analysis of IT standards and best practices (see footnote 1, page 18).

Universities are beginning to develop programs—ASU, UA, and NAU are in the early stages of developing their information security programs. Based on reviews of formalized and draft documents as well as statements by university officials, auditors determined that all three universities plan to incorporate an overall information security policy into their programs that will (1) establish university-wide commitment to information security and identify a governance structure and (2) include supplemental standards or procedures to provide guidance on how to implement key information security features such as risk assessment.

[1] For IT standards and best practices used, see footnote 1, page 18.

None of the universities have all needed information security program standards or procedures.

All three universities are in the process of developing supplemental standards or procedures to support their overall information security policy and key program features, but none have developed all the standards or procedures needed to support a complete information security program. Specifically,

- ASU has outlined the key features of its information security program, such as those listed in the textbox (see page 19), in a 5-year strategic plan draft, which auditors reviewed and found to be in line with IT standards and best practices; however, it is not yet final. ASU has also drafted an information security policy that auditors found to be in line with IT standards and best practices by establishing an overall governance structure; however, it is still a draft and has not yet been formally approved. Additionally, ASU is drafting various standards for its security program. However, as will be discussed in more detail below, the current program lacks adequate standards or policies for three of the four key features.

- UA officials stated that they do not intend to create a single document for the information security program, but will use different documents that when considered together will constitute the university's formal information security program. The documents include an overarching information security policy, several standards documents, and an IT Strategic Plan. Auditors found UA's information security policy, which received interim approval in February 2007 and final approval in April 2008, to be in line with IT standards and best practices as it provides an overall governance structure. Further, it has been disseminated through UA's Web site. In addition, UA's Information Technology Strategic Plan, which received approval in April 2008, indicates that UA is engaged in designing and implementing a comprehensive security program to protect sensitive information, reduce risk, and define roles and responsibilities. This plan has goals related to security and awareness and provides some limited information on all four of the key aspects of an information security program (see textbox, page 19). However, as will be discussed in more detail below, UA is lacking adequate standards or procedures for all four key features.

- NAU has outlined the features of its security program, such as those listed in the textbox (see page 19), in an information security policy and program document; its information security policy was approved in June 2005, and a document outlining its information security efforts was approved in October 2007. Auditors found that both the information security program and policy are in line with IT standards and best practices. According to an official, NAU also has various standards that are scheduled to be approved during the summer of 2008. However, as will be discussed in more detail below, NAU is lacking adequate standards or procedures for three of the four key features.

Universities should ensure programs include key security features

The information security programs at all three universities still lack adequate standards and procedures for most or all of the four key features listed in the textbox on page 19. As a part of their information security programs, the universities should continue their efforts to create and formalize procedures that address these four key security features.

Universities should establish a formal data classification process—None of the universities have a complete, finalized, university-wide data classification process. According to IT standards and best practices, a data classification process is critical to help ensure that sensitive data is identified and then protected based on risk, as well as to prevent unauthorized data access, modification, disclosure, and destruction. Additionally, data classification helps to ensure that universities meet statutory and regulatory requirements such as those regarding the privacy of student information.[1] IT standards and best practices indicate that data classification systems should include an overall classification process (see textbox).

Data Classification Process Criteria

An organization-wide data classification process should be established that:

- Protects information based on requirements such as confidentiality.
- Is reviewed and updated regularly.
- Consists of an inventory of information classification details that includes: classification, identity of the information owner, and a brief description of information classified.

Source: Auditor General staff analysis of IT standards and best practices (see footnote 1, page 18).

Although none of the universities have established a complete overall data classification process, each university is taking steps to address this area. For example, both ASU and UA have provided draft data classification documents as of February 26, 2008 and March 4, 2008, respectively. Both drafts, which have not yet been approved, require that the universities protect information based on requirements such as confidentiality. However, both drafts are missing key requirements. Specifically, neither draft requires the classifications to be reviewed and updated regularly, and ASU's draft does not require that an inventory (or equivalent) of information classification details be maintained. Therefore, ASU and UA need to improve their draft procedures for the data classification process to be in line with IT standards and best practices and then approve and implement them.

NAU has mapped out the data on its IT systems and university management indicated that this information will be used to continue its efforts to create a data classification process. However, to help ensure that sensitive data is properly protected, NAU should develop and implement a documented, university-wide classification process that is in line with IT standards and best practice requirements.

[1] For example, the Family Educational Rights and Privacy Act (FERPA) of 1974 governs the accessibility and privacy of student education records.

Universities should create formal risk assessment procedures—Risk

assessment, another key feature of an information security program, is not yet adequately in place at any of the three universities. According to IT standards and best practices, risk assessments are used in part to identify vulnerabilities within the organization, such as weak passwords or the lack of a plan for restoring IT or other business operations following a disaster, and determine what controls are needed to lessen the risk of someone exploiting those vulnerabilities. Without an effective risk analysis and assessment process, universities may not be able to adequately protect sensitive information or critical IT infrastructures by avoiding or reducing security threats, such as computer-assisted fraud, vandalism, and fire or flood. Risk assessments are also used to identify threats that originate outside of the university. Without a risk assessment, the universities may not be able to identify the controls needed to protect themselves against threats to sensitive data, such as malicious code, which is computer code that has been written to deliberately perform unauthorized functions, or computer hacking, which is gaining unauthorized access to computer systems for the purpose of stealing and corrupting data. IT standards and best practices state that there should be documented standards or procedures for performing regular information risk assessments that apply university-wide and mandate that the risk assessments be regularly performed (see textbox).

Risk Assessment Criteria

A documented organization-wide risk assessment process should be established that:

- Assigns responsibility.
- Mandates regular assessments.
- Consists of a structured methodology for assessing risks, including control weaknesses and operating/environmental threats.
- Documents results and potential impact of risks.
- Uses results to make changes to the security program and address risks.
- Reports results to top management.

Source: Auditor General staff analysis of IT standards and best practices (see footnote 1, page 18).

ASU, UA, and NAU each conducted a risk assessment in either late 2006 or early 2007 at the Arizona Board of Regent's (Board) request; however, none of the universities perform regular risk assessments university-wide. Although all three universities plan to perform risk assessments, only ASU has drafted a risk assessment standard at this time.

- ASU—In January 2008, ASU drafted a risk assessment standard that empowers the information security office to perform periodic risk assessments university-wide and explains the consequences for noncompliance. However, this standard has not yet been approved. ASU has also adopted an Information Risk Management Audit Check List, which, in line with IT standards and best practices, will help identify information security threats, controls, and weaknesses. In addition, according to an ASU official, ASU plans to develop a risk assessment process standard that will outline how risk assessments will be conducted and how the results will be documented and used. Therefore, ASU should obtain approval for its risk assessment standard and continue with its plans to develop and implement a risk assessment process standard.

- UA—Although UA officials indicated that they plan to perform risk assessments, no risk assessment policy, standards, or procedures have been developed. In May 2008, UA officials stated that the risk assessment process will be implemented by July 2009, and will include using an electronic tool for identifying vulnerabilities and developing plans to address the critical risks identified. According to IT standards and best practices, there are other elements involved in assessing risks, such as mandating regular assessments, and reporting results to upper management. Therefore, UA should continue its efforts to develop and implement risk assessment standards or procedures that are in line with IT standards and best practices.

- NAU—NAU's approved information security program document states that annual risk assessments will be performed beginning in the fall of 2008, but no risk assessment standards or procedures have been developed. In addition to the risk assessment conducted for the Board, NAU conducted a risk assessment in the spring of 2007. However, NAU still needs to create standards or procedures for how these assessments will be conducted and should ensure that its procedures are in line with IT standards and best practices.

Universities should enhance security awareness education and training—Although security awareness education and training is critical to help detect and avoid information security problems and incidents, ASU, UA, and NAU lack adequate, university-wide training programs. IT standards and best practices indicate that there should be a documented security awareness education and training program (or set of activities) that is mandatory for all individuals who have access to the organization's information and systems (see textbox). Without an effective security awareness program, universities may not be able to keep faculty, staff, and students aware of information security threats and concerns as well as their responsibilities and liabilities, or keep them equipped to support the university's security policy in the course of their normal work.

Although each university has taken some steps regarding security awareness, more needs to be done. For example, all of the universities have optional security awareness resources available to users through their Web sites, and ASU and UA also have other security awareness activities, such as security awareness days where information is available to faculty, staff, and students. However, these resources and activities do not constitute university-wide mandatory security awareness education and training that is geared toward an individual's role within the university as recommended by IT standards and best practices. Although the universities have mandatory training for some staff, the activities and training currently in use are not mandatory for every user. Therefore, the universities should take additional steps to establish university-wide security awareness education and training programs that are in line with IT standards and best practices including requiring security awareness education and training for all users, and gearing it toward their functions.

Security Awareness Education and Training Criteria

A documented organization-wide security awareness education and training program should be established that:

- Consists of awareness or training activities for all individuals with access to the organization's information or systems.
- Is geared toward the individual's role.
- Is mandatory, and kept up to date.
- Provides information that helps individuals understand: (a) the meaning of information security, (b) the importance of complying with information security policies, and (c) their responsibilities for information security (e.g. reporting actual and suspected incidents).

Source: Auditor General staff analysis of IT standards and best practices (see footnote 1, page 18).

Universities should finalize or improve their incident response procedures—ASU, UA, and NAU need to continue their efforts to develop and implement incident response processes that are in line with IT standards and best practices to ensure that information security events are reported and responded to as quickly as possible. According to IT standards and best practices, incident response is a process of detecting, reporting, and responding to information security incidents, such as a breach of confidential information because of a failure of IT security safeguards or computer hacking. It is important to respond quickly in order to minimize an incident's impact, such as a loss of revenue from computer-based university services while affected systems are identified, treated, and restored. In addition, effective incident response reduces the risk of similar incidents occurring and ensures that legal requirements are followed. For example, A.R.S. §44-7501 requires that any person or entity in Arizona holding computerized personal data should notify all affected parties if they determine there has been a security breach in which unauthorized access to unredacted or unencrypted personal information has occurred.

Incident Response Criteria

A standardized, documented, organization-wide process for managing information security incidents should be established that:

- Identifies roles and responsibilities.
- Provides the responding individuals with the authority to make critical decisions.
- Provides information on how to identify, respond to, recover from, and follow up on information security incidents.

Source: Auditor General staff analysis of IT standards and best practices (see footnote 1, page 18).

IT standards and best practices indicate that there should be a standardized, documented, organization-wide process for managing individual information security incidents (see textbox). Without adequate incident response standards and procedures in place, the universities cannot ensure that incidents are responded to consistently and effectively.

ASU, UA, and NAU need to finalize or improve their incident response standards or other documents. Specifically:

ASU's and NAU's draft incident response documents are in line with IT standards and best practices.

- ASU's draft Incident Response Plan, provided to auditors in January 2008, is in line with IT standards and best practices. Therefore, ASU should approve and implement its plan.

- UA has an approved information security policy, incident-handling standard, and incident-handling guideline, and although these documents contain some important information about UA's incident response process, they are not fully in line with IT standards and best practices. For example, UA's documents include some information on how to identify incidents such as how to be alert for or detect incidents, and how to report incidents. However, the information contained in the policy, standard, and guideline on how to report incidents is not consistent. For example, the security policy indicates that all incidents of actual or suspected compromise must be reported immediately to the University Information Security Officer (UISO). However, the standard gives users several different options for reporting incidents and reporting them to the UISO is not one of them. In addition, none of UA's documents clearly indicate a fundamental aspect of an incident response process that is in line with IT standards and best practices—identifying roles and responsibilities. UA's documents also do not have adequate information on how to respond to an incident once it is reported, such as how to investigate or contain the incident; and how to recover from or follow up on the incident, such as rebuilding systems and conducting a root cause analysis. Therefore, UA should ensure that its incident-handling documents include all key requirements outlined in IT standards and best practices, and that the information within these documents is consistent.

- NAU's December 2005 draft Computer Security Incident Response Team policy, along with its incident response guidelines and flowcharts, constitute an incident response process in line with IT standards and best practices. Therefore, NAU should approve and implement its incident response policy, guidelines, and flowcharts.

Other actions needed

ASU, UA, and NAU should take two additional steps to ensure that sensitive information and systems are adequately protected. First, each university should identify the necessary resources for implementing its information security program. Second, the universities should continue with their plans to monitor university-wide program compliance.

Universities should determine resources needed—None of the universities have yet determined the specific resources that will be needed to implement their information security programs, in part because each of the universities is in the early stages of implementing a formal information security program. ASU and UA officials believe they need additional resources for the ISOs to fulfill all of their necessary responsibilities associated with developing and implementing a university-wide information security program. In addition, according to an NAU official, additional full-time equivalent (FTE) positions could be used to reduce the time needed to fully implement the program. NAU's Information Technology Services requested and was granted additional funding for fiscal year 2008 to improve its information security efforts. However, it has not yet identified the specific resources it needs to implement other features of the information security program. In line with the Board's proposed IT policies and guidelines, ASU, UA, and NAU should determine their resource needs for implementing a formal information security program. In doing so, each university should assess whether it internally has the resources needed to develop and implement the program or whether it needs to develop a request for additional funding.

Universities should continue with plans to monitor program compliance—IT standards and best practices indicate that one of the ISO's key responsibilities is to monitor information security program compliance through reviews or audits, including monitoring university departments' compliance with the policies, procedures, and standards that have been established to ensure sensitive information and systems are properly protected. None of the universities have begun to monitor compliance with their information security programs, in part because each university is in the process of implementing its formal information security program, as previously mentioned. However, each university has plans for monitoring compliance.

- An ASU official stated that the university plans to monitor compliance by first conducting initial risk assessments to identify high-risk systems, and then conducting more detailed assessments of those high-risk systems. According to the official, ASU plans to have the initial risk assessments completed by July 31, 2008 (see pages 22 through 23 for more information on risk assessments).

- According to a UA official, UA plans to monitor compliance through risk assessments. Specifically, using an electronic tool, units will be directed to respond to a series of questions that will help determine whether they are in compliance with UA policies and standards and meet best practices.

- NAU intends to use its security analyst to conduct spot-checks or audits of information reported by its departments in response to a risk assessment questionnaire that will help determine the risks associated with the departments' systems and information, such as the type of information stored in the departments' systems and the types of controls that the departments have in place to protect sensitive information and systems.

Therefore, ASU, UA, and NAU should continue to develop and implement plans for monitoring compliance.

Universities should work with the Board—Because the Board oversees and assists the universities with IT security issues, ASU, UA, and NAU should work with the Board's Technology Oversight Committee (Committee) to establish timelines for implementing the audit recommendations. The universities should also regularly report to the Committee on the progress of their implementation efforts.

Recommendations:

1. ASU, UA, and NAU should:

   a. Seek additional opportunities while implementing their information security programs to ensure that their ISOs' authority is communicated and understood university-wide.

   b. Take additional steps to establish a university-wide security awareness education and training program that is in line with IT standards, including requiring security awareness education and training for all users and gearing it toward their functions.

   c. Determine their resource needs for implementing a formal information security program. In doing so, they should assess whether they internally have the resources needed to develop and implement their programs, or whether they need to develop a request for additional funding.

   d. Continue to develop and implement plans for monitoring information security program compliance.

   e. Work with the Board's Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

2. ASU should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by:

   a. Obtaining approval for its information security policy and Information Security and Privacy Strategic Plan, and then disseminating and communicating this policy to all appropriate individuals.

   b. Updating its university-wide data classification procedures to include creating an inventory and regularly reviewing and updating the classifications, and then approving and implementing the procedures.

   c. Obtaining approval for its risk assessment standard, and continuing with its plans to develop and implement a risk assessment process standard.

   d. Approving and implementing its incident response plan.

3. UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by:

   a. Improving its university-wide data classification procedures to require that classifications be regularly reviewed and updated, and then approving and implementing the procedures.

   b. Continuing its efforts to develop and implement risk assessment procedures that are in line with IT standards and best practices.

   c. Ensuring that its incident handling documents include all key requirements outlined in IT standards and best practices, and that the information within these documents is consistent.

4. NAU should continue its efforts to implement an information security program that is in line with IT standards and best practices by:

   a. Developing and implementing a documented university-wide data classification process in line with IT standards and best practices, such as protecting the information based on confidentiality, and developing an inventory of its data classification that is updated regularly.

   b. Developing and implementing university-wide risk assessment procedures in line with IT standards and best practices.

   c. Approving and implementing its incident response policy, guidelines, and flowcharts.

AGENCY RESPONSE

ASU
ARIZONA STATE UNIVERSITY

June 11, 2008

Debbie Davenport
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

On behalf of Arizona State University (ASU), I am pleased to respond to the performance audit regarding the Information Technology Security Program at ASU. ASU is in agreement with your recommendations and responses specific to your recommendations are enclosed. The report represents a thoughtful analysis of the ASU Information Technology Security Program.

ASU is very appreciative of the professional manner in which the audit was performed. We are always seeking to identify new and better ways to improve our programs and operations. The implementation of your recommendations will meaningfully enhance the Information Technology Security Program at ASU.

Sincerely,

Michael M. Crow
President

MMC:dq
/c

Enclosure

c: Adrian Sannier, Vice President, University Technology Officer
Carol Campbell, Executive Vice President and CFO

Response From Arizona State University

To the Auditor General's Report on

Information Technology Security

FINDING 1

1. ASU, UA, and NAU should:

   a) Develop and implement a plan for conducting regular security assessments of their Web-based applications.

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

   STATUS: ASU is actively developing a comprehensive strategy for assessing Web-based applications. In addition to collaborating with NAU and UA to deploy a common assessment tool set, ASU is leveraging industry standard methodologies for assessment around Web development and development in general practices and procedures.

   b) Enhance or develop and implement University-wide standards or procedures for updating and maintaining their Web servers.

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

   STATUS: ASU has created standards and procedures based on its Web-based applications. Implementation of these standards will be done in conjunction with training around secure coding practices. ASU's approach is to first create standards on the Operating System (OS), all Web browsers, and application servers, to be followed by development and maintenance standards for its Web applications and Java 2 Platform Enterprise Edition (J2EE) Web applications. To update and maintain Web servers, ASU and UTO will create procedures on best practices to support the recommendation.

   c) Establish and implement a set of University-wide standards for developing secure Web-based applications. These standards should encompass all phases of development.

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

   STATUS: ASU is implementing standards for Secure Software Development Lifecycles (SDLC) that will address all Web-based applications. ASU is focusing its initial implementation on its most critical enterprise systems. ASU will then apply these same standards University-wide.

d) Provide guidance and training to Web developers on secure Web-based development practices as part of a wider security awareness education and training effort.

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

STATUS: As part of ASU awareness and training, ASU is identifying mandatory training collateral that will be useful in training its Web-developer community. This material will be generally available beginning in Fall 09.

e) Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

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

STATUS: ASU has and will continue to work with the Arizona Board of Regents Technology Oversight Committee to report on all of its technology activities, including those related to information security.

FINDING 2

1. ASU, UA, and NAU should:

a) Seek additional opportunities while implementing their information security programs to ensure that their ISOs' authority is communicated and understood University-wide.

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

STATUS: ASU continues to articulate the role of the ISO through its various committees and counsels and the role and responsibilities of the ISO across the University.

b) Take additional steps to establish a University-wide security awareness education and training program that is in line with IT standards, including requiring security awareness education and training for all users and gearing it toward their functions.

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

STATUS: ASU has defined and is preparing to implement a University-wide awareness and training program. The “Get Protected” campaign is interactive and includes user-specific, mandatory courses on training and awareness education.

c) Determine their resource needs for implementing a formal information security program. In doing so, they should assess whether they internally have the resources needed to develop and implement their programs, or whether they need to develop a request for additional funding.

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

STATUS: ASU initially specified (3) FTEs and has currently filled one of these positions. ASU has also defined a budget for FY09 for resources, systems, applications, and awareness and will begin to track and manage expenditures for security program efforts.

d) Continue to develop and implement plans for monitoring information security program compliance.

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

STATUS: ASU’s Information Security Office is engaged with ASU’s Internal Audit team to develop and implement a program compliance plan. Over time, this responsibility will reside within the ISO’s Office.

e) Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

RESPONSE: ASU agrees with this finding of the Auditor General and is taking steps to implement it.

STATUS: ASU has and will continue to work with the Arizona Board of Regents Technology Oversight Committee to report on all of its technology activities, including those related to information security.

2. ASU should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by:

a) Obtaining approval for its Information Security Policy and Information Security and Privacy Strategic plan, and then disseminating and communicating this policy to all appropriate individuals.

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

STATUS: ASU is currently working with various committees and entities within the University to obtain approval for its draft Information Security Policy and Privacy Strategic plan.

b) Improving and implementing University-wide data classification procedures that are in line with IT standards and best practices, such as creating an inventory.

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

STATUS: ASU has begun a data classification investigation that will identify what types of data exist within the University systems and help focus security efforts on the most sensitive areas. In addition, there is an overall standard for data classification and management that is currently under review, as well as a set of best practices and procedures for protecting data of various classifications.

c) Obtaining approval for its risk assessment standard and continuing with its plans to develop and implement a risk assessment process standard.

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

STATUS: ASU has completed its initial risk assessment and has developed a schedule and plan for future assessments. ASU's ISO will leverage the Internal Auditing group to provide the initial functionality until the Information Security Office has established its own capability.

d) Approving and implementing its incident response plan.

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

STATUS: ASU has created and corrected issues within its Incident Response Plan and is working to ensure that it is maintained, updated, and evaluated on a consistent level.

THE UNIVERSITY OF ARIZONA®

Office of the President

Administration Building, Room 712
1401 E. University Boulevard
P.O. Box 210066
Tucson, AZ 85721-0066
Tel: (520) 621-5511
Fax: (520) 621-9323

June 13, 2008

FEDEX AIRBILL NUMBER 7920 7072 2217

Debra K. Davenport, CPA
Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Re: The University of Arizona

Dear Ms. Davenport:

Thank you for the opportunity to respond to the report issued in connection with the performance audit of information technology security at The University of Arizona (UA). We appreciate the professional approach of the auditors during their review. The purpose of this letter is to forward UA's written responses to the report.

UA's five-year information technology strategic plan identifies information technology security as a priority. Many improvements have been implemented. We welcomed the Auditor General's review as a means to enhance and refine our efforts.

UA agrees with the findings in the report and has implemented or plans to implement the recommendations as described in the accompanying report.

Sincerely,

Robert N. Shelton
President

RNS/slh

c: Michele Norin, Chief Information Officer and
Executive Officer for University Information Technology Services
Floyd Roman, Assistant Comptroller, Financial Management,
Financial Services Office
Sylvia Johnson, University Information Security Officer

THE UNIVERSITY OF ARIZONA RESPONSE TO INFORMATION TECHNOLOGY SECURITY PERFORMANCE AUDIT REPORT

Finding 1 – Universities need to improve Web-based application security

Finding 1, Recommendation 1a:

UA should develop and implement a plan for conducting regular security assessments of its Web-based applications. This plan should include:

- Creating and regularly updating an inventory of Web-based applications and determining the criticality of the applications and the data processed.
- Developing and implementing procedures for regularly conducting security reviews that assess whether security requirements and controls are functioning effectively.
- Remediating, based on risk, the problems identified during these security reviews.

UA Response:

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

UA's plan for conducting regular security assessments of Web-based applications is as follows:

- UA will inventory Web-based applications and the data processed and determine their criticality as part of UA's risk assessment process at least every three years.
- UA, ASU and NAU are in the process of acquiring Web application and network vulnerability scanning tools.
- UA central security staff will attend vendor-provided training covering all aspects of the scanning tools.
- Following completion of the vendor training, central security staff will begin training UA system administrators.
- Following completion of the vendor training, UA central security and UA IT staff will begin use of the tools to identify Web servers and assess security of Web-based applications.
- UA will develop and implement a procedure for regular security reviews and remediation of identified problems.

Finding 1, Recommendation 1b:

UA should enhance or develop and implement university-wide standards or procedures for updating and maintaining its Web servers. The standards or procedures should include:

- Developing a method for identifying relevant, widely known Web server vulnerabilities.
- Creating a timeline for reacting to notifications of newly discovered Web server vulnerabilities.

- Developing a process for determining whether to apply a software update, establish another control to address the Web server vulnerability, or accept the risk of not updating the software.

UA Response:

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

UA will use network vulnerability tools to identify Web server vulnerabilities on an ongoing basis.

UA will develop and implement a procedure that reinforces its Server Security Standard by identifying a method for identifying relevant, widely known Web server vulnerabilities, creating a timeline for reacting to notifications of newly discovered Web server vulnerabilities, and describing a process for determining whether to apply a software update, establish a compensating control, or accept the risk of not updating the software.

.

Finding 1, Recommendation 1c:

UA should establish and implement a set of university-wide standards for developing secure Web-based applications. These standards should encompass all phases of development and include:

- Gathering security requirements.
- Developing a set of up-to-date secure coding standards or conventions.
- Using threat modeling exercises during development.
- Performing security testing before releasing an application to the live environment.

UA Response:

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

UA will establish and implement a set of university-wide standards for developing secure Web-based applications.

Finding 1, Recommendation 1d:

UA should provide guidance and training to Web developers on secure Web-based development practices as part of a wider security awareness education and training effort.

UA Response:

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

The Information Security Office will continue to enhance the information for application developers currently available on its website.

UA will provide training for a number of its Web developers. Following completion of the training, trained Web developers will develop a sustainable training program for other UA Web developers.

Finding 1, Recommendation 1e:

UA should work with the Arizona Board of Regents' Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report its implementation efforts.

UA Response:

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

Finding 2 – Universities need to develop comprehensive IT security programs

Finding 2, Recommendation 1a:

UA should seek additional opportunities while implementing its information security program to ensure that its ISO's authority is communicated and understood university-wide.

UA Response:

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

In addition to steps already being taken, UA's ISO will:

- Establish an information security advisory committee, as required by the ABOR Information Security Policy, and periodically report to the Faculty Senate Executive Committee.
- Seek additional opportunities to meet with a variety of UA organizations.

Finding 2, Recommendation 1b:

UA should take additional steps to establish a university-wide security awareness education and training program that is in line with IT standards, including requiring security awareness education and training for all users and gearing it toward their functions.

UA Response:

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

The Information Security Office will continue to identify needs for training. Current efforts include:

- Planning the Information Security Office's sixth annual awareness event, with tracks for all types of users
- Development of new employee and refresher training to meet the mandate of UA's Standard on Management Responsibilities for Information Security
- Presentation of internal firewall implementation and management training sessions geared toward system administrators in May 2008, with the video version available on the Information Security Office website by July 2008
- Delivery of awareness education to over 6,000 incoming freshmen through new student orientation
- Delivery of awareness presentations to classes attended by one-third of UA's freshman class

Finding 2, Recommendation 1c:

UA should determine its resource needs for implementing a formal information security program. In doing so, it should assess whether it internally has the resources needed to develop and implement its program, or whether it needs to develop a request for additional funding.

UA Response:

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

UA will determine whether it has the internal resources needed to develop and implement its program over the next six months and, if it determines that it does not, will develop a request for additional funding. In making such a determination, UA will take into consideration the timelines developed in conjunction with the Arizona Board of Regents' Technology Oversight Committee, as described below.

Thereafter, any additional need for funding will be articulated in the information security program plan submitted annually to ABOR in accordance with the ABOR Information Security Policy.

Finding 2, Recommendation 1d:

UA should continue to develop and implement plans for monitoring information security program compliance.

UA Response:

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

Compliance will be monitored as part of the risk assessment process and by means of network vulnerability and Web application scanning.

Finding 2, Recommendation 1e:

UA should work with the Arizona Board of Regents' Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report its implementation efforts.

UA Response:

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

Finding 2, Recommendation 3a:

UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by improving its university-wide data classification procedures to require that classifications be regularly reviewed and updated, and then approving and implementing the procedures.

UA Response:

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

The data classification procedures will be revised by December 2008 to require the regular review and update of classifications. Approval of the procedures will be sought immediately after their revision.

Finding 2, Recommendation 3b:

UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by continuing its efforts to develop and implement risk assessment procedures that are in line with IT standards and best practices.

UA Response:

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

The Information Security Office will continue efforts to develop and implement university-wide risk assessment procedures in line with IT standards and best practices by July 2009.

Finding 2, Recommendation 3c:

UA should continue its efforts to develop and implement an information security program that is in line with IT standards and best practices by ensuring that its incident handling documents include all key requirements outlined in IT standards and best practices, and that the information within these documents is consistent.

UA Response:

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

The Incident Handling Standard and the Incident Handling Guideline have been implemented and have been available on UA's website since May 2006. Since their publication, the reporting of incidents at UA has increased significantly. UA will continue its efforts to raise awareness of information security matters, including the Incident Handling Standard and the Incident Handling Guideline.

UA's incident handling documents will be revised by December 2008 to:

- Ensure consistency
- Identify roles and responsibilities
- Incorporate additional detail on how to investigate or contain and recover from or follow up on incidents

NORTHERN
ARIZONA
UNIVERSITY

Office of the President

Northern Arizona University
PO Box 4092
Flagstaff, AZ 86011-4092

928-523-3232
928-523-1848 fax
nau.edu/president

June 11, 2008

Ms. Debra Davenport
Auditor General
State of Arizona
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

We have received the Auditor General's report on information technology security at the three state universities. Northern Arizona University has no significant issues or concerns with the report.

Attached is Northern Arizona University's response. The audit recommendations will be implemented.

Sincerely,

John D. Haeger
President

Northern Arizona University
Auditor General's Performance Audit
Information Technology Security
June 2008

Finding 1 - Universities need to improve Web-based application security

Recommendation a.

Develop and implement a plan for conducting regular security assessments of their Web-based applications

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. One of the primary responsibilities of the Information Security Analyst, Sr. position is to manage the security assessment program at NAU. Additionally, the Arizona Board of Regents Technology Oversight Committee approved funding for a suite of software applications to be used in the regular assessment of Web-based applications.

Recommendation b.

Enhance or develop and implement university-wide standards or procedures for updating and maintaining their Web servers.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. A university-wide standard or procedures for updating and maintaining web-servers will be developed and implemented.

Recommendation c.

Establish and implement a set of university-wide standards for developing secure Web-based applications.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. Information Technology Services has begun prototyping and testing a software development lifecycle standard. As this prototype matures it will be tested by others responsible for developing web-based applications on the campus. After it has been thoroughly reviewed it will be distributed as a university-wide standard.

Recommendation d.

Provide guidance and training to Web developers on secure Web-based development practices as part of a wider security awareness education and training effort.

Response

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

The first training for secure web-based development practices was held on May 20-May 23. This training was attended by twenty core web-application developers. The core developers receiving this training will be used in a train-the-trainer type effort to structure future training opportunities for the campus.

Additionally, on-going guidance will be developed and distributed to campus-wide web-application developers based on the standards developed in response to Recommendation c and updates to best practices in web-application development.

Recommendation e.

Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The NAU Director of Information Security will work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and providing progress reports.

Finding 2 - Universities need to develop comprehensive IT security programs

Recommendation 1a.

Seek additional opportunities while implementing their information security programs to ensure that their ISO's authority is communicated and understood university-wide.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The Director of Information Security will work with the NAU Information Security Committee to identify campus organizations for targeted awareness efforts to this effect.

Recommendation 1b.

Take additional steps to establish a university-wide security awareness education and training program that is in line with IT standards, including requiring security awareness education and training for all users and gearing it toward their functions.

Response

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

Work has begun in coordination with the Director of Human Resources and the NAU Training Coordinator to gain approval for a suite of mandatory training for faculty, staff, and students at NAU.

An annual schedule for training and awareness has been developed and presented to the NAU Information Security Committee. The first monthly training was held on April 23 and awareness articles were included in the ITS newsletter.

The Information Security Awareness coordinator at the University of Arizona has been contacted to begin arranging for the purchase of professional security awareness materials to be distributed at NAU.

Recommendation 1c.

Determine their resource needs for implementing a formal information security program. In doing so, they should assess whether they internally have the resources needed to develop and implement their programs, or whether they need to develop a request for additional funding.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The approved NAU Information Security Program calls for an annual risk assessment to be conducted. One aspect of the risk analysis is an assessment of resources needed to mitigate risks. This assessment will be completed this fall per the Program, and will assess whether there are enough internal resources to develop and implement the program, or whether a request for additional funding is required.

Recommendation 1d.

Continue to develop and implement plans for monitoring information security program compliance.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. A plan for monitoring compliance with the information security program will be developed and implemented.

Recommendation 1e.

Work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and regularly report their implementation efforts.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The NAU Director of Information Security will work with the Arizona Board of Regents Technology Oversight Committee to establish timelines for implementing audit recommendations and providing progress reports.

Recommendation 4.

NAU should continue its efforts to implement an information security program that is in line with IT standards and best practices by:

Recommendation 4a.

Developing and implementing a documented university-wide data classification process in line with IT standards and best practices, such as protecting the information based on confidentiality, and developing an inventory of its data classification that is updated regularly.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. A university-wide data classification process will be developed and implemented.

Recommendation 4b.

Developing and implementing university-wide risk assessment procedures in line with IT standards and best practices.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. An initial inventory and assessment was conducted in 2007. Part of that assessment lead to the approval of the NAU Information Security Program. The Program calls for an annual risk assessment to be completed each fall. A draft risk assessment strategy has been developed and will provide the foundation for these assessments.

Recommendation 4c.

Approving and implementing its incident response policy, guidelines, and flowcharts.

Response

The finding of the Auditor General is agreed to and the audit recommendation will be implemented. The incident response policy, guidelines, and flowcharts are being reviewed and approval will be sought for their campus-wide implementation.

ARIZONA
BOARD OF
Regents

Arizona Board of Regents
2020 North Central Avenue, Suite 230
Phoenix, AZ 85004-4593
602-229-2500
Fax 602-229-2555
www.azregents.edu

Arizona State University ***Northern Arizona University*** ***University of Arizona***

June 13, 2008

Ms. Debra Davenport
Auditor General
State of Arizona
2910 North 44th Street, Suite 410
Phoenix, AZ 85018

Dear Ms. Davenport:

Thank you for the opportunity to review the revised preliminary performance audit report of information technology security at the Arizona public universities.

We appreciate the professionalism of your staff and their responsiveness to our earlier comments.

While the report does not include any specific recommendations directed to the Arizona Board of Regents, we will work with the Board and the universities to ensure progress in implementing the recommendations directed to the universities.

Sincerely,

Joel Sideman
Executive Director

c:
Regent Fred Boice
Art Ashton
Rick Gfeller

Performance Audit Division reports issued within the last 24 months

06-04	Arizona Department of Education—Accountability Programs
06-05	Arizona Department of Transportation—Aspects of Construction Management
06-06	Arizona Department of Education—Administration and Allocation of Funds
06-07	Arizona Department of Education—Information Management
06-08	Arizona Supreme Court, Administrative Office of the Courts—Information Technology and FARE Program
06-09	Department of Health Services—Behavioral Health Services for Adults with Serious Mental Illness in Maricopa County
07-01	Arizona Board of Fingerprinting
07-02	Arizona Department of Racing and Arizona Racing Commission
07-03	Arizona Department of Transportation—Highway Maintenance
07-04	Arizona Department of Transportation—Sunset Factors
07-05	Arizona Structural Pest Control Commission
07-06	Arizona School Facilities Board
07-07	Board of Homeopathic Medical Examiners
07-08	Arizona State Land Department
07-09	Commission for Postsecondary Education
07-10	Department of Economic Security—Division of Child Support Enforcement
07-11	Arizona Supreme Court, Administrative Office of the Courts—Juvenile Detention Centers
07-12	Department of Environmental Quality—Vehicle Emissions Inspection Programs
07-13	Arizona Supreme Court, Administrative Office of the Courts—Juvenile Treatment Programs
08-01	Electric Competition
08-02	Arizona's Universitities—Technology Transfer Programs
08-03	Arizona's Universities—Capital Project Financing

Future Performance Audit Division reports

Arizona Biomedical Research Commission

Arizona Board of Podiatry Examiners