Arizona's Universities
Information Technology Security

Universities have implemented several information technology (IT) security practices and can further improve IT security, policies, procedures, and practices

Performance Audit

June 2018
Report 18-104

A Report to the Arizona Legislature

Lindsey Perry
Auditor General

ARIZONA Auditor General
Making a Positive Difference

ARIZONA Auditor General

Making a Positive Difference

The Arizona Office of the Auditor General's mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, the Office provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Representative **Anthony Kern**, Chair
Representative **John Allen**
Representative **Rusty Bowers**
Representative **Rebecca Rios**
Representative **Athena Salman**
Representative **J.D. Mesnard** (ex officio)

Senator **Bob Worsley**, Vice Chair
Senator **Sean Bowie**
Senator **Judy Burges**
Senator **Lupe Contreras**
Senator **John Kavanagh**
Senator **Steve Yarbrough** (ex officio)

Audit Staff

Dale Chapman, Director
Jeff Gove, Manager and Contact Person
Melinda Gardner, Manager

Brian Miele, Team Leader
Diana Boatwright
Michael A. Castle
Katie Morris
Gina Pascua
Lisa Webster
Kristi Wisdom

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

LINDSEY PERRY, CPA, CFE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

June 21, 2018

Members of the Arizona Legislature

The Honorable Doug Ducey, Governor

Mr. John Arnold, Interim Managing Director
Arizona Board of Regents

Dr. Michael M. Crow, President
Arizona State University

Dr. Rita Hartung Cheng, President
Northern Arizona University

Dr. Robert C. Robbins, President
The University of Arizona

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 A.R.S. §41-1279.03. I am also transmitting within this report a copy of the Report Highlights for this audit to provide a quick summary for your convenience.

As outlined in their responses, the Arizona Board of Regents, Arizona State University, Northern Arizona University, and the University of Arizona agree with all of the findings and plan to implement or implement in a different manner all of the recommendations.

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

Sincerely,

Lindsey Perry, CPA, CFE
Auditor General

cc: Arizona Board of Regents members

Attachment

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


ARIZONA
Auditor General
Making a Positive Difference

ARIZONA Auditor General
Making a Positive Difference

REPORT HIGHLIGHTS
Performance Audit
June 2018

Arizona's Universities
Information Technology Security

CONCLUSION: Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA) have implemented several information technology (IT) security practices consistent with IT standards and best practices, but these practices can be improved. Specifically, relatively few university employees were susceptible to our simulated social engineering attacks, but some employees took actions that could have provided an attacker with access to sensitive data, indicating a need to improve security awareness training. In addition, although the universities' security controls limited our attempts to gain unauthorized access to their IT systems, we were able to exploit some vulnerabilities to access sensitive data. The universities should enhance their existing policies and procedures in five key areas to further reduce these potential vulnerabilities. Further, each university has established components of an IT security governance framework, but NAU and UA should continue to develop and implement their frameworks. The Arizona Board of Regents (ABOR) should also expand its oversight of the universities' IT security efforts. Finally, each university can improve its data classification processes, and NAU and UA should improve their IT risk assessment and incident response processes.

Universities responsible for safeguarding IT systems and data

ASU, NAU, and UA use computerized electronic systems to support numerous functions such as payroll and student admission applications. To perform these functions, the universities use IT systems to store and process various types of sensitive data, including social security numbers, financial and health information, and educational records for approximately 34,000 faculty and staff, approximately 161,000 students, some of the more than 850,000 alumni, and others, such as prospective students applying for admission. The volume of sensitive data the universities obtain and maintain makes them a potential target for attacks by malicious individuals or organizations, and federal and state laws and regulations specify the universities' responsibility in handling and protecting sensitive data.

Universities should improve security awareness training efforts and enhance IT security controls to further protect IT systems and data

Relatively few employees susceptible to simulated social engineering attacks but security awareness training efforts can be improved—Social engineering attacks attempt to persuade an entity's employees to provide information about, or direct access to, the entity's network using specially crafted means. Although a relatively small number of university employees were susceptible to our simulated social engineering attacks, some employees disclosed information or took other actions that could have provided an attacker with unauthorized access to the universities' IT systems and sensitive data. For example, one attack strategy provided us the means to potentially access IT systems and sensitive data at ASU and UA, and information obtained through another attack strategy allowed us to gain unauthorized access to NAU's internal network, which could have allowed us to potentially view, modify, or delete sensitive student information. Information security awareness training is important for reducing successful social engineering attacks. Although each university requires their employees to complete some security awareness training, not all university employees have done so. Specifically, as of March 2018, training completion rates were 68 percent at ASU, and as of April 2018, 61 percent at NAU, and 40 percent at UA. The lack of completed training at all three universities may have contributed to employees' susceptibility to simulated social engineering attacks.

Universities' security controls slowed simulated attacks, but vulnerabilities allowed unauthorized access to some IT systems and sensitive data—We conducted simulated attacks on the universities' IT systems, but our ability to gain unauthorized access to these systems was limited because the universities employ automated security tools and have separated portions of their respective networks into smaller, protected subnetworks. However, after ASU removed some controls to allow us to more quickly identify and exploit vulnerabilities, we gained unauthorized access to sensitive data at ASU, including names, contact information, and grades. At NAU, we identified some vulnerabilities that allowed us to gain unauthorized access to legally protected data such as records related to

medical issues. We also exploited vulnerabilities to gain unauthorized access to some IT systems and sensitive data at all three universities that could have led to university service disruptions and further attacks. For example, we gained the ability to enter and void transactions at a cash register at ASU, take control of an IT system that manages some water and electrical services at NAU, and upload malicious software to financial and administrative systems at UA. Although all three universities have established policies and procedures for five key IT security controls that help prevent or detect unauthorized access to IT systems and data—vulnerability management, configuration management, patch management, web application development, and log monitoring—weaknesses in these IT security controls contributed to the vulnerabilities we identified and exploited.

Recommendation

ASU, NAU, and UA should improve their security awareness training compliance and enforcement policies and procedures and, where appropriate, further strengthen and align their existing IT security policies and procedures with IT standards and best practices for vulnerability management, configuration management, patch management, web application development, and log monitoring.

NAU and UA should continue to improve and develop IT security governance frameworks and ABOR should enhance its IT security governance by expanding its oversight activities

NAU and UA can improve IT security governance frameworks—IT standards and best practices indicate that organizations should develop an IT security governance framework that includes several components, including an IT security strategic plan, documented roles and responsibilities, policies and guidance, and processes for monitoring the effectiveness of institutional IT security practices. ASU has developed an IT security governance framework that includes all four recommended components, whereas NAU has developed three of the four recommended components and UA has developed two of the four recommended components. However, some of the framework components developed by NAU and UA are not fully aligned with best practices.

ABOR can enhance its IT security governance by expanding oversight activities—Higher education governing boards play an important role in ensuring universities' IT security risks are adequately addressed by providing oversight. Although ABOR provides some IT security guidance and oversight to the universities, its oversight efforts do not include several recommended practices for providing effective IT security governance. Implementing these practices may have helped ABOR and the universities identify and address several of the IT security issues we identified.

Recommendations

NAU and UA should either continue developing or develop and implement IT security governance frameworks.

ABOR should expand its oversight of the universities' IT security efforts using existing processes.

Universities should improve processes in three key information security program areas

Although each university has either wholly or partially implemented appropriate data classification, risk assessment, and incident response processes, which are important for adequately protecting their IT systems and the data contained in them, each university should take steps to improve in one or more of these areas. For example, ASU's data classification policies and procedures do not include a requirement for its individual colleges, departments, and other business units to develop a data inventory as part of its data classification process; NAU has not yet implemented its data classification policies and procedures; and UA's data classification policy also does not include a requirement for individual units to develop a data inventory. Additionally, NAU and UA have not fully implemented their IT risk assessment policies and procedures. Finally, NAU's and UA's incident response policies and procedures do not include information about training or testing as recommended by IT standards and best practices.

Recommendation

Where appropriate, ASU, NAU, and UA should revise or develop and implement policies and procedures for data classification, risk assessment, and incident response.

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

Scope and objectives

The Office of the Auditor General has conducted a performance audit of information technology (IT) security at Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA) 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 final in a series of three performance audits of the State's universities. The first audit reviewed the universities' fee-setting processes, and the second audit reviewed the universities' processes and strategies for improving undergraduate retention and graduation rates.

Universities process, use, and store large volumes of sensitive data

The State's universities—ASU, NAU, and UA—obtain and maintain large volumes of sensitive data on their computerized electronic systems. Specifically, all three universities use electronic systems to support numerous functions such as payroll; student admission applications, academic progress, status, and financial aid; and university initiatives to increase student graduation and retention rates. To perform these functions, the universities use IT systems to store and process various types of sensitive data, including names, birthdates, social security numbers, financial and health information, and educational records for approximately 34,000 faculty and staff, approximately 161,000 students, some of the more than 850,000 alumni, and others, such as prospective students applying for admission.[1]

Universities are required to secure sensitive data

The volume of sensitive data that the universities obtain and maintain makes them a potential target for attacks by malicious individuals or organizations. Therefore, the universities have a responsibility to safeguard their systems and sensitive data from misuse or attack. Both federal and state laws and regulations specify the responsibility of universities in handling and protecting sensitive data. Specifically, the Family Educational Rights and Privacy Act requires the universities to keep student records private and to maintain a record of any instance of disclosure. Additionally, the Gramm-Leach-Bliley Act, which applies to specific financial activities, contains requirements for the security of financial data, including sending customers, such as students, a written notice of privacy policies and practices concerning data security. Further, the Arizona Board of Regents (ABOR), which is the governing body of the State's universities, has developed a policy manual that includes specific guidelines for the universities related to protecting sensitive data. For example, ABOR's policy manual states that each of the universities should establish procedures for the secure handling and storage of electronically stored information to prevent unauthorized access or misuse and includes requirements for developing additional controls for IT systems that process sensitive data.

Further, several laws require universities to notify affected individuals and organizations and other entities, such as the media, in the event of a data breach. For example, A.R.S. §18-545 requires that any person or entity in Arizona holding electronic personal data notify all affected parties if it determines there has been a security breach in which unauthorized access to unredacted or unencrypted personal information has occurred if that

[1] The approximate number of students is based on the universities' fiscal year 2017 full-time equivalent student enrollment, a statutorily mandated measure of student enrollment.

compromise places the affected parties at risk of economic loss.[2] Similarly, certain health-specific information, which some universities maintain, is subject to a notification requirement under HIPAA. In addition to notifying the affected individuals, HIPAA also requires the organization that experiences such a breach to notify the Secretary of the Department of Health and Human Services of the breach. Further, HIPAA requires that when an organization storing health information experiences a breach involving more than 500 residents of a state or jurisdiction, it must notify prominent media outlets serving the area. Finally, ABOR policy states that if a university determines that a security breach involving personal information has likely occurred, the university's Information Security Officer or Information Security Director should report the incident promptly and in writing to ABOR's chair and president.

Security attacks have exploited IT weaknesses in universities world-wide

Universities are subject to information security attacks that may lead to data breaches. Although each data breach is unique, attacks typically exploit IT security weaknesses that may be present in an organization's IT systems, networks, and environment. Attempts to compromise IT systems are not uncommon, and universities world-wide have been subject to large breaches. These breaches can have considerable costs to both the organizations that are breached and the individuals whose data is improperly accessed.

Security attacks exploit IT weaknesses—Security weaknesses can be exploited to gain access to and/or compromise IT systems and gain access to sensitive data. Although each security breach is unique, most attacks against IT systems follow a similar process. In most instances, security attacks include the following three general steps:

1. **Public information gathering—**An attacker will attempt to gather as much information about an entity as possible using public resources, such as information available through the internet, to focus attacks on weak points.

2. **IT system scanning—**An attacker will perform some direct probing steps to attempt to find weaknesses, such as scanning entity resources with automated tools.

3. **Exploiting—**An attacker will attempt to exploit weaknesses to obtain unauthorized access to an IT system.

These steps may be performed both externally and internally depending on the attacker, the attacker's goal, and the resources available. When performed with success, these steps may build on one another to allow an attacker to gain unauthorized access to an IT system. These steps may not always be performed in the order listed above and may be performed multiple times over an extended time period. Finally, attackers may use social engineering in tandem with these steps to convince users to provide them with information needed to obtain unauthorized access to IT systems (see Finding 1, pages 5 through 6, for more information on social engineering attacks).

Universities world-wide have experienced large data breaches—Each year, colleges and universities across the country are subject to large data breaches. According to the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization whose mission is to engage, educate, and empower consumers to protect their privacy and advocate for positive change, colleges and universities reported approximately 13 electronic breaches affecting over 540,000 records in 2016 and 2017 (see textbox, page 3, for examples of university data breaches).[3] Additionally, Symantec, a well-known IT security company, discovered over 350

---

[2] A.R.S. §18-545 does not apply to financial institutions obligated to protect nonpublic personal information of its customers per Title V of the federal Gramm-Leach-Bliley Act, covered entities as defined under the federal Health Insurance Portability and Accountability Act (HIPAA), the Arizona Department of Public Safety, county sheriffs' departments, municipal police departments, prosecution agencies, or courts because these entities must follow other notification procedures outlined in federal and state laws.

[3] Privacy Rights Clearinghouse reported that this number fluctuates as new breaches are identified and reported. Likewise, breaches may be reported without information on the number of people affected.

Examples of university data breaches

University of Maryland, College Park (UMCP)—In February 2014, a data breach occurred at UMCP that resulted in an unauthorized disclosure of personally identifiable information UMCP had stored. The breach involved over 280,000 faculty, students, staff, and affiliated personnel records. The records included individuals' names, birthdates, social security numbers, and student numbers. After discovering the breach, UMCP notified the Maryland Police Department of the data breach and university officials notified the public by establishing a data breach website with a letter from the university president. UMCP also attempted to notify those whose information was stolen, provided 5 years of opt-in credit-monitoring services to all affected individuals, created a cybersecurity task force to identify policies and procedures for ensuring future IT security, and corrected known system vulnerabilities.

University of Calgary—In May 2016, the University of Calgary was infected by ransomware that locked academic administrators and professors out of the school's digital network. Ransomware is software intended to block access to a computer system until the hackers who infected the system with the ransomware are paid a ransom to restore access. Once the ransom is paid, the hackers provide keys or other methods of decryption. The university paid the hackers a ransom of approximately 20,000 Canadian dollars to regain access to the system.

Michigan State University (MSU)—MSU reported that, in November 2016, an unauthorized party gained access to a university server containing sensitive data. The database contained approximately 400,000 records including names, social security numbers, student identification numbers, and in some cases student and employee birthdates. MSU reported that the unauthorized party accessed 449 of the records in the database. MSU offered 2 free years of identity theft protection, fraud recovery, and credit monitoring.

Source: Auditor General staff analysis of information primarily from the websites of the organizations that were breached and reports on these breaches.

new pieces of malware in 2016.[4,5] Finally, according to a March 2018 statement released by the United States Department of Justice, a series of coordinated email phishing attacks carried out by Iranian hackers between approximately 2013 and December 2017 compromised approximately 8,000 professors' email accounts across 144 U.S.-based universities and 176 universities located in other countries.[6] The hackers then used the stolen account information to obtain more than 31 terabytes of academic and intellectual property, including research, academic journals, theses, and dissertations, and then sold some of this information to others via the internet.[7] ASU, NAU, and UA reported that they had not been contacted by the United States Department of Justice to inform them whether they were among the affected universities.

Data breaches have considerable costs to both organizations and individuals—When data is improperly accessed through a security breach, both the organization that was breached and the individuals whose information was accessed can incur considerable costs. Ponemon Institute, an organization that conducts independent research on privacy, data protection, and information security policy, reported in its *2017 Cost of Data Breach Study: Global Overview* that the average cost of a breach in the United States was $225 per record accessed. World-wide, the fiscal year 2017 cost of a data breach averaged $141 per record accessed.[8] Further, individuals who have their information improperly accessed or stolen may spend time and resources monitoring

---

4 Symantec. (2017). *Internet security threat report, Vol. 22*. Mountain View, CA.

5 Malware is software intended to damage a computer, mobile device, or IT system; take control over its operation; or gather sensitive data. Malware can be used to facilitate a breach of an IT system.

6 Email phishing is a social engineering technique in which an attacker sends devious emails in an attempt to convince a user to click on a link to open an external connection the attacker may use to gain unauthorized access to an organization's IT system (see Finding 1, pages 5 through 6, for more information on social engineering).

7 A terabyte is approximately one trillion bytes, or 1,000 gigabytes, and is equivalent to approximately 86 million pages of text documents, or about 3.6 million images.

8 Ponemon Institute. (2017). *2017 cost of data breach study.* Traverse City, MI.

their credit and may become victims of identity theft. Organizations that experience data breaches could also lose credibility and suffer a damaged reputation.

Universities' IT staff, expenses, and organization

For fiscal year 2017, ASU, NAU, and UA reported that they collectively used more than 1,870 full-time equivalent (FTE) positions and $328 million for IT-related purposes system-wide. According to information each university provided, this included 962 FTEs and more than $178 million at ASU; 209 FTEs and more than $34 million at NAU; and 700 FTEs and more than $116 million at UA. University officials reported that IT-related expenses include staff salaries and benefits as well as costs to purchase and maintain IT software and hardware.

Each of the three universities has a central IT office with IT staff who are responsible for providing some services to the entire university. Each university employs a chief information officer (CIO) who is responsible for broad oversight of IT operations for the entire university.[9] Additionally, all three universities employ a chief information security officer who reports to the CIO and has responsibility for university-wide IT security and heads an information security office (ISO). In fiscal year 2017, the size of the ISO at each university varied with ASU reporting 19 FTE, NAU reporting 5 FTE, and UA reporting 2.71 FTE in their respective ISOs.

[9] UA also employs a Vice President for Information Strategy and University Libraries who oversees its CIO's activities.

Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Although relatively few university employees were susceptible to simulated social engineering attacks, these employees disclosed information or took other actions that could have provided an attacker with access to sensitive data, such as employee personnel records; therefore, the universities should enhance their security awareness training efforts to help further reduce the risk of successful social engineering attacks. Auditors simulated social engineering attacks targeting Arizona State University (ASU), Northern Arizona University (NAU), and University of Arizona (UA) employees, and a relatively small number of these employees were susceptible to the attacks, but those attacks allowed auditors to gain or potentially gain unauthorized access to the universities' information technology (IT) systems and the information contained in them, including sensitive data. To help further reduce the risk of successful social engineering attacks, the universities should improve their security awareness training efforts by developing policies and procedures for regularly tracking employees' compliance with training requirements and implementing enforcement mechanisms for employees who do not comply with those requirements.

University employees less susceptible to simulated social engineering attacks, but small number of successful attacks puts sensitive data at risk

Although relatively few university employees were susceptible to auditors' simulated social engineering attacks, these employees disclosed information and/or took other actions in response to these attacks that could have allowed an attacker to gain unauthorized access to sensitive data. Most attacks to exploit security weaknesses and gain access to and/or compromise IT systems include the following steps: gathering information, scanning IT systems to find weaknesses, and exploiting these weaknesses (see Introduction, page 2, for more information on these steps). In addition, attackers may use social engineering in tandem with these steps to convince users to provide them with information or the means needed to obtain unauthorized access to IT systems (see textbox on page 6 for more information on social engineering attacks). For example, as discussed in the Introduction (see page 3), Iranian hackers stole academic and intellectual property after using phishing emails to compromise email accounts of approximately 8,000 professors at 144 U.S.-based universities and 176 universities located in other countries.

Auditors used a number of social engineering techniques targeted at ASU, NAU, and UA employees and found that most employees were not susceptible to these attacks.[10] For example, ASU employees were not susceptible to one type of social engineering technique auditors used. In addition, the success rate for auditors' simulated attacks using a different social engineering technique at each university was less than half the percentage of

[10] Specific information about the security weaknesses identified and the methods used to identify them, such as the number of employees involved in auditors' simulated social engineering attacks, has been excluded from this report and shared only with appropriate university officials because of the sensitive nature of this information.

Social engineering—These attacks attempt to persuade an entity's employees to provide some information about, or direct access to, the entity's network using specially crafted means. Social engineering attacks may include:

- **Email phishing—**Sending specially crafted emails in an attempt to convince a user to click on a link to open an external connection that the attacker may use to gain unauthorized access.
- **Phone phishing—**Calling employees to persuade them to divulge sensitive information, such as personal information or their usernames and passwords.
- **Physical social engineering—**Attempting to convince employees at an entity to grant access to a physical building by playing a part or pretending to have the appropriate permission for access.

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

successful attacks outlined in a recent report where a similar attack method was used against educational institutions. Specifically, the reported percentage of successful attacks against educational institutions was 11 percent, while the success rates at ASU, NAU, and UA were less than 1 percent, nearly 2 percent, and approximately 4 percent, respectively.[11]

However, despite the relatively low success rates observed at the universities, auditors either gained or could have potentially gained unauthorized access to the universities' IT systems and sensitive data through the small number of successful simulated social engineering attacks. For example, one attack strategy provided auditors the means to potentially access certain IT systems and sensitive data at ASU and UA. In addition, using information obtained through another attack strategy, auditors were able to gain unauthorized access to NAU's internal network, which could have allowed auditors to potentially view, modify, or delete sensitive student information, such as names, addresses, financial aid data, and admissions data.

Universities should enhance their security awareness training efforts to further reduce success of social engineering attacks

Information security awareness training is important for reducing the success of social engineering attacks by helping employees understand the meaning of information security and techniques attackers use to try to compromise it, the risks inherent with information security, the importance of complying with information security policies, and their responsibilities for information security, such as not giving out their passwords over the phone or clicking links in potential phishing emails. IT standards and best practices indicate that organizations should define roles and responsibilities of staff who will develop and implement security awareness training materials, evaluate and update security awareness training materials, have processes to monitor compliance with and effectiveness of security awareness training efforts and requirements, use an automated tracking system to analyze and report on security awareness training efforts at an organization-wide level, and follow up with employees to take corrective action for addressing noncompliance.[12]

Although ASU, NAU, and UA each require their employees to complete some security awareness training and have taken or are taking steps to help ensure their employees complete this training, not all university employees are doing so. For example, as part of ASU's 2017 IT risk assessment process, ASU's individual units, such as academic colleges and departments, were asked to report the percentage of their employees who had completed required security awareness training. ASU reported that it plans to continue asking individual units to report this information during its 2018 and 2019 IT risk assessments (see Finding 4, pages 40 through 41, for more information on ASU's IT risk assessment process). Based on the results of its 2017 IT risk assessment, which indicated that many of its individual units had low security awareness training completion rates, ASU's Information Security Office identified security awareness training as a high-risk area of focus and recommended

[11] Cofense. (2017). *2017 enterprise phishing resiliency and defense report*. Leesburg, VA.

[12] Wilson, M., & Hash, J. (2003). *NIST Special Publication 800-50: Building an information technology security awareness and training program*. Gaithersburg, MD: National Institute of Standards and Technology.

that individual units that had deficiencies in this area take various actions, such as sending letters to remind employees to complete the training. Additionally, in March 2018, NAU developed a draft policy for security awareness training that requires NAU's Information Security Office to track and report employee training completion rates and follow up with individual units regarding employees who have not completed the mandatory training. Further, in December 2017, UA developed a security awareness training policy that outlines the UA staff who will be responsible for ensuring its security awareness training is completed and states that new employees who do not complete the required training within 60 days may lose access to UA's IT systems. However, despite these steps, not all university employees are complying with the universities' requirements to complete security awareness training. Specifically, as of March 2018, ASU reported that 68 percent of its employees had completed its security awareness training. In addition, as of April 2018, NAU reported that 61 percent of its employees had completed its security awareness training, while UA reported that 40 percent of its employees had completed its security awareness training. The lack of completed training at all three universities may have contributed to auditors' success using social engineering attacks.

To help ensure all required university employees complete security awareness training, the universities should enhance their security awareness training efforts. Specifically:

- **Universities should further enhance or, where needed, develop and implement security awareness training compliance and enforcement policies and procedures—**To help better ensure their employees complete required security awareness training, ASU, NAU, and UA should develop and implement the following security awareness training policies and procedures:

  - **ASU should develop and implement policies and procedures for monitoring security awareness training compliance—**Although ASU has developed some procedures for tracking and monitoring employee compliance with its security awareness training requirements, it has not established policies and procedures specifying roles, responsibilities, or requirements for using these procedures; has not established requirements for following up with employees who have not completed the training; and has not specified enforcement mechanisms that should be used. IT standards and best practices recommend that organizations develop formal security awareness training policies to help ensure that all employees complete this training. Therefore, ASU should develop and implement written policies and procedures that:

    - Specify roles and responsibilities for monitoring employee compliance with security awareness training requirements;

    - Include a requirement for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so;

    - Specify requirements for following up with employees who have not completed the required security awareness training; and

    - Identify potential consequences to employees for not completing required security awareness training within specified time frames, such as warnings and revoked access.

  - **NAU should complete the development of and implement its policies and procedures for ensuring security awareness training compliance—**NAU is in the process of developing security awareness training policies and procedures that specify roles and responsibilities for monitoring employee compliance with security awareness training requirements and identify potential consequences for employees who do not comply with these policies and procedures. However, although the draft policies and procedures indicate that NAU will track training completion rates and follow up with individual units that have employees who do not complete the training, they do not contain time frames or procedures for doing so. Therefore, NAU should finish developing and implement its draft security awareness training policies and procedures, including adding requirements for:

- Regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and

- Following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its draft security awareness training policies and procedures.

  - **UA should develop and implement procedures for ensuring security awareness training compliance—**UA developed a security awareness training policy in December 2017 that assigns responsibility for ensuring employee compliance with security awareness training requirements to the employees' supervisors and identifies potential consequences to employees for not completing required training. However, UA has not developed policies or procedures for regularly monitoring training compliance and following up with employees who do not complete required training. Therefore, UA should develop and implement additional policies or procedures for:

    - Regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and

    - Following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its security awareness training policy.

- **NAU and UA should further align their security awareness training policies and procedures with best practices—**IT standards and best practices recommend that organizations provide security awareness training to new employees as part of initial training and to existing employees at least annually thereafter. NAU and UA should align their policies and procedures accordingly, as follows:

  - **NAU should specify a time frame for completing initial security awareness training—**NAU's draft security awareness training policy requires existing NAU employees to complete security awareness training annually and requires new NAU employees to complete initial security awareness training when they are hired; however, it does not specify a time frame for completing this initial training. Therefore, NAU should specify a time frame for new employees to complete initial security awareness training within its policies and procedures.

  - **UA should require annual security awareness training for existing employees and periodically update training materials—**Although UA's security awareness training policy specifies that existing employees may be required to periodically complete security awareness training, it does not make this a requirement, nor does it specify a time frame for periodically completing training, such as annually. Further, UA's security awareness training policy does not define roles and responsibilities of staff who will develop and implement security awareness training materials, nor does it include requirements or guidance for evaluating and updating security awareness training materials. Therefore, UA should revise its security awareness training policies and procedures to require existing employees to complete security awareness training annually, define the roles and responsibilities of staff who will develop and implement security awareness training materials, and include requirements for periodically evaluating and updating security awareness training materials.

Recommendations

1.1. ASU should develop and implement written policies and procedures that:

a. Specify roles and responsibilities for monitoring employee compliance with security awareness training;

b. Include a requirement for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so;

c. Specify requirements for following up with employees who have not completed the required training; and

d. Identify potential consequences to employees for not completing required security awareness training within specified time frames, such as warnings and revoked access.

1.2. NAU should finish developing and implement its draft security awareness training policies and procedures, including adding requirements for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its draft security awareness training policies and procedures.

1.3. NAU should specify a time frame for new employees to complete initial security awareness training within its policies and procedures.

1.4. UA should implement its security awareness training policy and develop and implement additional policies or procedures for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its security awareness training policy.

1.5. UA should revise its security awareness training policies and procedures to require existing employees to complete security awareness training annually, define the roles and responsibilities of staff who will develop and implement security awareness training materials, and include requirements for periodically evaluating and updating security awareness training materials.

Universities should enhance IT security controls to further protect IT systems and data

The State's universities—Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA)—have established various information technology (IT) security controls but can strengthen these controls to help ensure that their IT systems and the data contained in them, including sensitive data such as social security numbers and confidential health information, are protected from unauthorized access. Auditors conducted simulated attacks on the universities' IT systems and found that the universities' IT security controls generally helped block and/or slow down attempts to exploit security weaknesses; however, auditors were able to exploit some vulnerabilities to gain access to and compromise IT systems and gain access to sensitive data. To better protect their IT systems and sensitive data, the universities should further align their IT security policies and procedures with IT standards and best practices in five IT security control areas, including vulnerability management and web application development. In addition, to help ensure their IT systems and sensitive data are consistently protected, the universities should each develop and implement a process for addressing identified instances of noncompliance with their IT security policies and procedures.

Universities' security controls slowed simulated attacks, but vulnerabilities allowed unauthorized access to some IT systems and sensitive data

Although auditors' ability to gain unauthorized access to the universities' IT systems and data was limited, auditors were able to exploit IT security weaknesses, or vulnerabilities, to access some of the universities' IT systems and sensitive data. Auditors conducted limited attack simulations on each of the universities' networks and at least five high-risk web applications at each university (see textbox for information on web applications).[13] Two common factors at the universities helped block and/or slow auditors' attempts to gain unauthorized access to their IT systems and data. Specifically:

A **web application** is a software program or IT system that is accessed by an end user to perform a transaction with a web browser, such as Internet Explorer or Chrome, over a network such as the internet. An external web application is accessible from any user device connected to the internet and could be more susceptible to attack.

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

- **Automated security tools blocked some attacks—**The universities employ automated security tools, including intrusion prevention/detection systems and antivirus software, which in some instances blocked auditors' simulated attempts to exploit known vulnerabilities that had been identified by software vendors and other individuals or organizations and published on the internet or in publicly available vulnerability databases. Intrusion prevention/detection systems block known security vulnerabilities and monitor network traffic for suspicious activity and issue alerts when such activity is discovered, and antivirus software can detect, block, and isolate malicious programs and files an attacker uploads to a network before they cause harm.

[13] Auditors' simulated attacks were limited in scope because auditors used a risk-based approach to test only a portion of each university's network and selected a small number of identified vulnerabilities to test within a limited time frame. See the Introduction, page 2, for more information on common attack patterns. Specific information about the security weaknesses identified and the methods used to identify them has been excluded from this report and shared only with appropriate university officials because of the sensitive nature of this information.

- **Network complexity and segmentation helped slow attacks—**Each university has a complex network consisting of numerous IT systems with many connections to each other, which made it more difficult for auditors during their simulated attacks to traverse the network and gain access to multiple systems. In addition, all three universities have segmented their networks, or separated portions of the network into smaller subnetworks or segments, and protected these segments to help ensure only authorized users have access to these areas of the network. These segmented networks further limited auditors from unauthorized movement across the universities' networks.

However, auditors identified and exploited vulnerabilities to gain unauthorized access to some of the universities' IT systems and sensitive data contained in them, such as educational records, medical documents, and information about IT systems that could allow attackers to conduct further attacks. Specifically:

- **Sensitive data in web applications accessed—**Auditors identified vulnerabilities in web applications that could have allowed attackers to gain unauthorized access to sensitive data at ASU, NAU, and UA. At ASU, auditors exploited a vulnerability and obtained unauthorized access to sensitive data on hundreds of thousands of individuals, including names, addresses, phone numbers, grades, grade point averages, and other information. Auditors exploited the vulnerability after ASU had removed some controls to provide auditors more access to the web application. Removing controls is a common practice during penetration testing (see page 13 for information on penetration testing) to help penetration testers more quickly identify and exploit vulnerabilities during simulated attacks. Although ASU's controls would have slowed down an attacker, they would not necessarily have prevented an attacker from identifying the vulnerability and obtaining sensitive data. At NAU, auditors exploited a vulnerability and obtained unauthorized access to thousands of legal documents and unauthorized access to legally protected and sensitive data such as records related to medical issues.[14] At UA, auditors identified various vulnerabilities that could have provided access to sensitive information about some web applications and potentially compromised them.

  Auditors promptly notified the universities of the vulnerabilities. ASU and NAU immediately fixed their respective vulnerability and reported that they had reviewed their activity logs to confirm that there were no other instances of unauthorized access on the web applications during the time that their respective vulnerability existed (see pages 19 through 20 for more information about activity logs). In addition, UA staff reported that they immediately began to address their vulnerabilities.

- **IT systems and sensitive data accessed, creating the potential for disruptions and further attacks—**Auditors exploited vulnerabilities to gain unauthorized access to some IT systems and sensitive data at all three universities that could have led to university service disruptions and further attacks. For example, auditors gained the ability to enter and void transactions at a cash register at ASU, take control of an IT system that manages some water and electrical services at NAU, and upload malicious software to financial and administrative systems at UA. In addition, auditors gained access to—and sometimes control over—IT systems at all three universities, such as security cameras, printers, and other systems. By gaining unauthorized access to these IT systems and the data contained in them, auditors could have disrupted university services; viewed, modified, or deleted information such as security camera footage and documents sent to printers; and gained access to other IT systems connected to these systems. Further, auditors obtained user names and passwords and other information that could have provided access to IT systems on the universities' networks and the data contained in these systems.

Although eliminating all vulnerabilities may not be possible, the universities should take steps to reduce the number of vulnerabilities in their IT systems and networks by improving policies and procedures in five IT security control areas discussed in the next section.

[14] NAU staff reported that the vulnerability auditors exploited was the result of an oversight by one of NAU's vendors. In addition, NAU staff reported that in the event of a real attack, NAU's controls may have impeded an attacker's ability to gain access to the web application.

Universities should improve policies and procedures for five IT security controls

Although all three universities have established policies and procedures for IT security in five key areas that help prevent or detect unauthorized access to IT systems and data, the universities should improve these policies and procedures. Specifically, weaknesses in the universities' vulnerability management, configuration management, patch management, web application development, and log monitoring processes contributed to the vulnerabilities identified and exploited during auditors' limited attack simulations. Therefore, ASU, NAU, and UA should strengthen their policies and procedures in these five IT security control areas by taking steps to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate (see textbox for more information on risk-based approaches for IT security).[15]

Risk-based approaches for implementing IT security controls

Because organizations may have limited resources for protecting their IT systems and data, IT standards and best practices indicate that organizations can take risk-based approaches for implementing IT security controls. Risk-based approaches involve addressing items classified as higher-risk more frequently, more extensively, and/or before addressing lower-risk items. However, a risk-based approach should also address lower-risk items because risk classifications may change over time and some higher-risk items may be misclassified as low-risk. Additionally, attackers can still leverage low-risk items to gain unauthorized access to IT systems and data.

Source: Auditor General staff analysis of IT standards and best practices from various sources.

All three universities should further align vulnerability management policies and procedures with IT standards and best practices—Vulnerability management is the process of identifying vulnerabilities, or IT security weaknesses; evaluating the associated risks of these vulnerabilities; and either correcting or mitigating the risk of the vulnerabilities or documenting the acceptance of risk. Vulnerability management includes similar activities for identifying vulnerabilities as those conducted during auditors' simulated attacks on the universities' IT systems (see textbox for the three general activities of a vulnerability management process). Organizations can identify and address some vulnerabilities, such as configuration and patch-related vulnerabilities (see pages 16 through 18 for more information on configuration and patch management), including those caused by policy noncompliance, by regularly scanning and remediating all IT systems on their networks and web applications.

All three universities conduct some vulnerability management activities, but these activities have not ensured that all vulnerabilities that can lead to unauthorized access to IT systems and data, including sensitive data, have been remediated. Specifically, auditors conducted scanning and penetration testing to identify and exploit several vulnerabilities and gained unauthorized access to IT systems and obtained information that could have led to further attacks and access to other IT systems and sensitive data. Although all three universities' vulnerability management processes include some of the components recommended by IT standards

Vulnerability management involves three general activities:

- **Scanning—**The use of automated tools to identify vulnerabilities within IT systems, including IT networks and web applications.
- **Penetration testing—**The process of simulating attacks on IT systems using manual and automated processes to systematically identify potential vulnerabilities across the IT environment, attempt to gain access to systems and data by exploiting these vulnerabilities, and then document the testing results in a comprehensive report.
- **Remediation—**The process of reviewing and addressing identified vulnerabilities or formally accepting their associated risks, such as when business needs outweigh security requirements.

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

[15] Auditors reviewed IT standards and best practices from the National Institute of Standards and Technology and the Open Web Application Security Project. See Appendix A, page a-1, for specific citations.

and best practices, these processes are missing some components, which may have contributed to auditors' ability to identify and exploit vulnerabilities. As a result, the universities should take the following steps to improve their vulnerability management processes:

- **ASU should ensure it conducts sufficient scans and penetration tests at appropriate intervals—**ASU generally performs vulnerability scans and penetration testing on its network and in web applications. However, ASU's vulnerability management processes:

  - **Lack comprehensive scanning policies and procedures to ensure its network is thoroughly scanned at appropriate intervals—**ASU scans some of the IT systems on its network and its web applications and has developed some related policies and procedures that are aligned with IT standards and best practices. However, ASU's policies and procedures are not comprehensive. Specifically, although these policies and procedures include requirements to scan ASU's web applications, including specifying which web applications will be scanned and the frequency with which these scans should occur, they do not include similar requirements for scanning the IT systems on ASU's network. In addition, ASU officials reported that ASU does not scan some of the IT systems on its network or many of its web applications and has not documented why they are not required to be scanned. Further, ASU has not always scanned its web applications within the time frames its policy specifies (see page 21 for more information). Finally, ASU's policies and procedures do not require scan results to be shared across the university to help eliminate similar vulnerabilities in other IT systems, as recommended by IT standards and best practices.

  - **Do not include penetration testing policies and procedures to ensure an appropriate risk-based approach—**ASU performs penetration testing on some of the IT systems on its network and its web applications but lacks associated policies and procedures for doing so. As a result, ASU has not specified how often penetration testing should occur, as recommended by IT standards and best practices. In addition, although ASU staff indicated that they take a risk-based approach to select applications for penetration testing, this approach is not documented. Further, although IT standards and best practices indicate that high-risk IT systems should have regular penetration testing, in calendar years 2016 and 2017, ASU conducted penetration tests on only 62 percent of its web applications that it identified as high risk.

  Therefore, ASU should develop and implement written policies and procedures for its vulnerability management process that include requirements and/or guidance for:

  - Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual departments, colleges, or business units (units) are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;

  - Sharing scan results across the university to help eliminate similar vulnerabilities in other IT systems;

  - Conducting penetration testing at specified frequencies based on risk;

  - Using its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and

  - Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

- **NAU should complete and implement its vulnerability scanning policy and develop and implement policies and procedures for penetration testing—**NAU performs monthly vulnerability scans of most

of the IT systems on its network and its web applications. Although NAU staff have followed informal guidance to conduct scanning, NAU had not officially documented its scanning processes until March 2018. Specifically, as of March 2018, NAU developed draft vulnerability management and scanning policies and procedures aligned with IT standards and best practices that were in the final stages of approval. Additionally, although NAU performs penetration testing and reported that it uses a risk-based approach to determine which network IT systems and web applications to test, NAU has not developed written penetration testing policies and procedures that define which systems should be tested and the required time frames for doing so, as recommended by IT standards and best practices. As a result, NAU may not be conducting sufficient penetration testing to adequately identify potential security weaknesses. For example, in calendar year 2017, NAU conducted manual penetration tests that included comprehensive assessments and reports of only 1 percent of its web applications that it identified as higher risk. However, in calendar year 2017, NAU also contracted with a third party to conduct security scanning and testing of its external web applications that included some common penetration testing elements, and some of NAU's high-risk web applications were included in the testing.[16]

To help ensure vulnerabilities in its network and web applications are effectively identified and addressed, NAU should finish developing and implement its draft policies and procedures establishing a vulnerability scanning process. Additionally, NAU should develop and implement written university-wide policies and procedures for penetration testing that include:

- Requirements for conducting penetration testing at specified frequencies based on risk;
- Guidance for its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and
- Guidance for helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope of, or frequency of, penetration tests for some or all higher-risk web applications.

- **UA should ensure it conducts sufficient scans and penetration tests at appropriate intervals—**UA scans only a portion of the IT systems on its network, does not scan web applications, and does not conduct penetration testing. Specifically:
  - **UA's network scanning is limited, and it does not scan web applications—**Although UA has scanning policies and procedures, these policies and procedures do not require all of UA's IT systems on its network to be scanned, thus increasing the potential that vulnerabilities may not be detected. Additionally, a UA official reported that UA does not scan its web applications even though UA's policies and procedures require annual web application scanning. Further, IT standards and best practices recommend that organizations analyze scan results and share these results across the organization to help eliminate similar vulnerabilities in other IT systems, but a UA official reported that some of its scan results are not being analyzed and therefore cannot be shared across the university.
  - **UA does not conduct penetration testing—**UA does not perform penetration testing for the IT systems on its network or its web applications. In addition, UA has not developed penetration testing policies and procedures that define which systems should be tested and the required time frames for doing so, as recommended by IT standards and best practices.

  Therefore, UA should develop and implement written policies and procedures for its vulnerability management process that include requirements and/or guidance for:

[16] Although the third party provided NAU with information related to vulnerabilities in NAU's web applications, NAU reported that the third party did not provide NAU with any reports to demonstrate the full extent of its scanning and testing, such as a listing of all the systems that it scanned.

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;

- Analyzing scan results, including specifying time frames for conducting the reviews, and sharing these results across the university to help eliminate similar vulnerabilities in other IT systems;

- Conducting penetration testing at specified frequencies based on risk;

- Using a risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and

- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

All three universities should align configuration management policies and procedures with IT standards and best practices—Configuration management is the process of ensuring IT systems have appropriate configurations, or settings that control how these systems operate, to maintain the integrity of information on these systems. For example, configuration management could include specifying the software that is appropriate to install on a server versus an individual computer or workstation or which applications should or should not be run on an IT system. When IT systems are not properly configured, errors may occur, system functionality may be inhibited, and these systems may be more susceptible to attacks.

Although all three universities have established some configuration management policies and procedures, configuration-related vulnerabilities on the universities' IT systems have not been adequately addressed. Specifically, during limited attack simulations, auditors identified configuration-related vulnerabilities on network servers at all three universities, some of which were exploited to gain unauthorized access to IT systems and to obtain information that could have led to further attacks. Auditors scanned the universities' networks for critical, high-, medium-, and low-risk vulnerabilities and identified the following:

- Of the 18,214 ASU servers and devices scanned, 6,737 had potential configuration-related vulnerabilities (approximately 37 percent);

- Of the 8,524 NAU servers and devices scanned, 485 had potential configuration-related vulnerabilities (approximately 6 percent); and

- Of the 10,622 UA servers and devices scanned, 5,692 had potential configuration-related vulnerabilities (approximately 54 percent).

Each university's configuration management policies and procedures lack some recommended elements to help ensure their IT systems are configured consistent with best practices, which may have contributed to the vulnerabilities auditors identified. Specifically, contrary to recommended IT standards and best practices, all three universities' policies and procedures do not include:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions; or

- Requirements for developing baseline configurations, which provide a standard set of specifications for configuring an IT system.

In addition, all three universities do not specify how often to review and update IT system configurations as recommended by IT standards and best practices. Further, all three universities' processes for configuring some of their IT systems contained common settings that, if not individualized or randomized, could provide potential

attackers with a means to move from system to system more easily. Therefore, some critical settings should be made unique to limit broad access that could result from keeping common settings in place. Finally, NAU's policies do not apply to all its IT systems, potentially leaving some of its IT systems more vulnerable to attack.

Therefore, ASU, NAU, and UA should develop and implement revised configuration management policies and procedures consistent with each of these IT standards and best practices. Additionally, NAU should revise its configuration management policies and procedures to indicate that they apply to all NAU IT systems.

Universities should take various steps to improve their patch management processes— Hardware and software vendors periodically issue updates, or patches, to their products to correct security vulnerabilities and other system flaws they have identified to improve the security, usability, and performance of their products. Patch management is the process of identifying patches that have been issued by these vendors, establishing a plan to apply them, and applying them, as appropriate.

The universities have each established some patch management processes. However, auditors scanned the universities' networks for critical, high-, medium-, and low-risk vulnerabilities and identified the following:[17]

- Of the 18,214 ASU servers and devices scanned, 746 had potential patch-related vulnerabilities (approximately 4 percent);
- Of the 8,524 NAU servers and devices scanned, 163 had potential patch-related vulnerabilities (approximately 2 percent); and
- Of the 10,622 UA servers and devices scanned, 617 had potential patch-related vulnerabilities (approximately 6 percent).

Auditors exploited several of these vulnerabilities to gain unauthorized access to IT systems and to obtain information that could have led to further attacks.

Although the universities' patch management policies and procedures include several components recommended by IT standards and best practices, they are missing some components, which may have contributed to the identified vulnerabilities. As a result, the universities should improve their patch management processes, as follows:

- **ASU's patch management policies and procedures should incorporate one additional best practice component—**ASU has developed patch management policies and procedures that are generally aligned with IT standards and best practices. These policies and procedures require all devices on ASU's network to be patched at defined time periods once the patch has been released and tested. However, they do not include guidance on how its staff should identify system flaws that require a patch and to whom these flaws should be reported once they are identified, as recommended by IT standards and best practices. As a result, not all system flaws may be identified and reported to those who are responsible for applying the necessary patches. Therefore, ASU should develop and implement additional patch management policies and procedures to include guidance on how its staff should identify system flaws requiring patches and requirements for reporting those flaws to appropriate individuals for remediation.
- **NAU should finish developing and implement its draft patch management policies and procedures—** During the audit, NAU staff reported that for some systems, they did not have a process to validate whether patches had been properly installed and did not use its IT system that provided reports and alerts indicating when patches were missing or improperly installed. Additionally, NAU lacked a policy to develop risk-mitigation strategies for devices that can no longer be patched, such as devices that need to be decommissioned because they use software that is no longer supported by a vendor. However, as of March 2018, NAU had developed draft patch management policies and procedures that were aligned with IT standards and best practices and were in the final stages of approval. For example, these draft policies and procedures include

[17] Patches are generally given a severity rating based on the level of risk posed by the associated vulnerability. For example, a patch may be rated high-risk if the associated vulnerability could result in compromised confidential user data.

guidance on identifying, reporting, testing, and installing patches within defined time periods. NAU should finish developing and implement these draft patch management policies and procedures.

- **UA's patch management policies and procedures should incorporate several best practice components—**Although UA has developed patch management policies and procedures, they lack several recommended components. For example, UA's policies and procedures do not include guidance on how its staff should identify system flaws that require a patch and to whom these flaws should be reported once they are identified; do not require patches to be tested for effectiveness and potential side effects before installation; and do not outline required time frames for installing patches. Therefore, UA should develop and implement patch management policies and procedures that include the following:
    - Identifying needed patches, reporting those patches to appropriate individuals responsible for remediation, and applying patches;
    - Testing patches for effectiveness and potential side effects before installation; and
    - Installing patches within required time frames.

All three universities should further align web application development policies and procedures with IT standards and best practices—According to IT standards and best practices, incorporating security into the web application development process is more cost effective and secure than applying security fixes afterward. To help facilitate secure web application development, IT standards and best practices recommend that organizations follow five security-related practices during the web application development process (see textbox for information on these five practices). In addition, IT standards and best practices state that staff who are responsible for developing IT systems should receive training on how to build secure software, such as web applications.

As previously discussed (see page 12), auditors were able to exploit vulnerabilities in some web applications to gain unauthorized access to sensitive data at ASU and NAU. In addition, auditors identified some common security vulnerabilities in all the web applications tested at all three universities that could have been used for further attacks. Although all three universities have developed policies and procedures for web application development, these policies and procedures lack some of the security-related components recommended by IT standards and best practices, which may have contributed to these vulnerabilities. Specifically:

- ASU's web application development policies and procedures do not include any criteria or guidance for using secure coding standards when developing web applications. Additionally, ASU's policies and procedures recommend, but do not require, source code review for web applications prior to release. Further, although ASU's policies and procedures require staff to perform security testing on higher-risk web applications before

When developing web applications, organizations should:

- **Gather security requirements—**Security requirements should include classifying data in the application according to its level of confidentiality and defining how the web application will comply with all relevant regulations and standards related to this data;
- **Use up-to-date secure coding standards—**These are steps that should be followed to develop a web application based on best practices;
- **Perform threat modeling during development—**Threat modeling involves defining 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;
- **Review source code—**Source code review is the process of manually checking the source code of a web application for security issues that may not be detected with any other form of analysis or testing; and
- **Perform security testing before releasing a web application to the live environment—**Conducting security testing, such as scanning or penetration testing, before release helps ensure that web-based applications function as intended and do not contain vulnerabilities when released.

Source: Open Web Application Security Project. (2014). *Testing guide, version 4.0*. Bel Air, MD: OWASP Foundation.

releasing them to the live environment, the policies and procedures recommend, but do not require, security testing for low-risk web applications. Finally, although ASU's policies and procedures recommend that new and significantly modified web applications be reviewed by professionally trained staff, they do not include training requirements for ASU's web application developers.

- NAU's web application development policies and procedures do not include any criteria or guidance for gathering security requirements. In addition, these policies and procedures do not provide guidance for using some up-to-date secure coding standards when developing web applications and do not include training requirements for NAU's web application developers. Further, NAU's policies and procedures lack requirements to conduct threat modeling during web application development to identify potential vulnerabilities or to conduct security testing before releasing web applications to the live environment. Finally, although NAU's web application guidelines indicate that source code from web applications developed by third-parties or other outside sources should be checked for known vulnerabilities and potentially modified if vulnerabilities are discovered, NAU does not require this type of review for the web applications it internally develops.

- UA's web application development policies and procedures do not include any criteria or guidance for reviewing source code and performing security testing before releasing web applications to the live environment. Finally, UA staff reported that web application developers do not receive training on securely coding web applications.

A 2008 Office of the Auditor General performance audit similarly found that vulnerabilities existed in the universities' web applications and recommended that the universities establish and implement university-wide standards for developing secure web applications consistent with IT standards and best practices (see Report No. 08-04). Although the universities took some steps to address these recommendations, these efforts were not sustained. Therefore, the universities should develop and implement web application development policies and procedures consistent with each of the previously discussed IT standards and best practices, as applicable.

All three universities should further align their log monitoring policies and procedures with IT standards and best practices—Collecting and monitoring logs of critical IT system activities enables organizations to track events on IT systems and to detect improper actions by any person who may access its IT systems, whether staff or nonstaff. For example, logs may track logins and connections to critical applications, systems, and devices, as well as changes to data and data transfer activities. IT standards and best practices recommend organizations establish a log monitoring process that includes the following:

- Describes the IT systems and functions within each IT system that should be logged;

- Specifies how frequently each log should be monitored;

- Identifies who is responsible for ensuring log events are captured and reviewing log events on a regular basis;

- Analyzes security-related information generated by log monitoring across an organization to determine any patterns that might indicate a potential attack;

- Develops standard response actions for specific types of detected events, including informing designated personnel of security risks to the university and to individual IT systems; and

- Includes requirements for securely protecting the logs, including protecting them from unauthorized access, modification, and deletion, and time frames for how long to retain the logs before deleting them.

Both ASU and UA have established log monitoring policies and procedures that align with some IT standards and best practices, but these policies and procedures are missing some best practice components. Additionally, although NAU has developed some log monitoring processes, it has not established written policies and procedures outlining these processes. Therefore:

- **ASU should establish one additional log monitoring best practice—**ASU has established log monitoring policies and procedures that are generally consistent with IT standards and best practices. However, these

policies and procedures do not outline how system logs should be protected from unauthorized access, modification, and deletion. Therefore, ASU should develop and implement policies and procedures for protecting system logs from unauthorized access, modification, and deletion.

- **NAU should develop and implement written log monitoring policies and procedures—**As of March 2018, NAU had implemented four automated systems that facilitate a log monitoring process for some of NAU's IT systems, including generating daily system log reports and alerts that identify some types of potentially suspicious activities. However, NAU has not developed written policies and procedures for using these four systems for log monitoring purposes, which should include the log monitoring processes previously mentioned, such as specifying critical IT system activities that should be logged and monitored, time frames for how frequently each log should be monitored, and requirements for securely protecting and retaining the logs as recommended by IT standards and best practices. Therefore, NAU should develop and implement written log monitoring policies and procedures for all its IT systems consistent with IT standards and best practices.

- **UA should further align its log monitoring policies and procedures with IT standards and best practices—**Although UA has log monitoring policies and procedures, these policies and procedures are not fully aligned with IT standards and best practices. For example, the policies and procedures do not include how frequently each log should be monitored. Additionally, UA staff indicated that they review logs only if they become aware of a problem rather than proactively monitoring logs, as recommended by IT standards and best practices. Further, UA has not clearly identified who is responsible for capturing and reviewing logs on a regular basis or how UA will monitor its logs to identify university-wide patterns that might indicate a potential attack. Finally, UA does not have procedures for securely protecting the logs or designating time frames for how long to retain log events before deleting them for some IT systems. Therefore, UA should develop and implement policies and procedures that address each of these log monitoring standards and best practices.

Universities should address noncompliance with IT security policies and procedures

ASU, NAU, and UA should each take steps to address instances of noncompliance with IT security policies and procedures. As discussed in Finding 3 (see pages 29 through 32), several individual units—such as academic colleges and departments—at all three universities are responsible for implementing university-wide IT security policies and procedures. Specifically, all of ASU's 33 reported individual units, 10 NAU individual units, and all of UA's 63 reported individual units are responsible for implementing university-wide IT security policies and procedures, although these units may rely to some extent on staff in their university's respective central IT office to implement policies and procedures on their behalf.[18] However, auditors reviewed some individual units' implementation of their respective university's policies and procedures for the five IT security areas previously discussed and identified several instances where university staff did not follow existing university policies and procedures, were unaware that they were responsible for implementing these policies and procedures, and/or did not know that university-wide policies and procedures existed.[19] Auditors also found instances where university staff in central IT offices did not follow university policies and procedures. For example:

- **Some ASU staff did not follow university-wide vulnerability scanning and log monitoring policies—**Some ASU staff in its University Technology Office (UTO)—which is responsible for developing and operating IT at ASU—and in individual units did not follow ASU's policies and procedures. Specifically:

[18] NAU's Information Technology Services department is responsible for implementing NAU's IT security policies and procedures for most of NAU's 224 reported individual units, but 10 individual unit leaders, including college deans and department directors, have this responsibility for their units (see Finding 3, page 30, for additional information).

[19] Auditors judgmentally selected 1 of 18 ASU individual units and 1 of 10 NAU individual units that officials at each respective university identified as operating to some extent independently from their respective central IT offices, which are responsible for university-wide IT development and operation. Auditors randomly selected 6 of UA's 63 reported individual units because all individual units at UA operate relatively independently of UA's central IT office. See Appendix A, page a-1, for auditors' methodology for selecting the sample of individual units.

- ASU policy requires all high-risk web applications to be scanned every 6 months. However, during calendar year 2017, ASU's UTO did not scan 2 of ASU's 41 high-risk web applications and scanned 3 of its 41 high-risk web applications only once instead of the required two times.[20] Further, ASU policy requires higher-risk vulnerabilities to be remediated within specified time frames, depending on the severity of the vulnerability, but ASU staff have not always followed this policy.

- ASU staff in one unit reported that they monitored logs only after an issue was identified instead of periodically monitoring logs to identify potential issues, which includes daily monitoring of higher-risk systems, as required by ASU's log monitoring policy.

- **Some NAU staff were not aware of existing university-wide secure web application development policies and procedures—**The one NAU unit auditors reviewed had its own web application developers, but unit management indicated that the unit did not have any policies and procedures for securely developing web applications. In addition, the unit management was unaware of NAU's secure web application development policies and procedures. Further, staff in NAU's Information Technology Services department—which is responsible for the development and operation of IT at NAU—were also unaware of these policies and procedures. As a result, NAU has not ensured that all staff follow its secure web application development policies and procedures when developing its web applications.

- **Some UA staff were not aware of scanning responsibilities, had not established configuration management procedures, and had not followed a web application assessment policy—**Staff in 3 of 6 UA units auditors reviewed stated that they believed UA's University Information Technology Services (UITS) office—which is responsible for developing and operating IT at UA—automatically scanned their networks, but UITS office staff stated that they scan the individual units' servers only upon a unit's request. As a result, UITS was not scanning these 3 individual units' servers. In addition, although UA's individual units are required to implement university-wide IT security policies, at least 2 of the 6 UA units reviewed had not developed configuration management procedures for implementing UA's university-wide configuration management policy. Further, UA staff in its Information Security Office (ISO)—which is responsible for overseeing UA's IT security efforts—did not follow UA's procedure for assessing the effectiveness of web application security requirements and controls, which includes several requirements such as updating UA's web application inventory and conducting network and application scans for IT systems containing web applications.

Therefore, ASU, NAU, and UA should take steps to help ensure that all their respective university staff are aware of and follow university-wide IT security policies and procedures. Internal control standards developed by the U.S. Government Accountability Office recommend organizations develop processes for reporting policy compliance issues to those responsible for implementing and overseeing policies, evaluating these issues, and completing and documenting corrective actions or exceptions to policy compliance within specified time frames.[21] As discussed in Finding 3 (see page 30), ASU has developed monitoring processes to identify noncompliance with its IT security policies and procedures. In addition, NAU and UA plan to develop and implement similar processes to identify noncompliance with their IT security policies and procedures (see Finding 3, pages 31 through 34). Therefore, in conjunction with monitoring efforts described and/or recommended in Finding 3, and to help ensure identified instances of noncompliance with IT security policies and procedures are adequately addressed, ASU, NAU, and UA should develop and implement university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementing and overseeing IT security policies and procedures;

---

[20] ASU reported that two of the high-risk web applications that were scanned only once should have been exempted from its policy, but ASU did not formally approve policy exemptions for these two web applications until May 2018. In addition, ASU indicated that a vendor that is responsible for one of the web applications that was not scanned during 2017 had a security certification that provided assurance of the security controls in place for the web application. However, ASU policy does not state that security certifications can be used in lieu of scanning, and as of May 2018, ASU had not formally approved a policy exemption for this web application.

[21] U.S. Government Accountability Office. (2014). *Standards for internal control in the federal government*. Washington, DC.

- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

Finally, UA should take steps to ensure its individual units have sufficient guidance to implement its IT security policies. Specifically, UA has developed university-wide IT security policies and procedures, but UA's individual units are responsible for implementing these policies and procedures and can develop their own additional procedures to supplement the university-wide policies and procedures. However, UA's university-wide IT security policies and procedures in the five areas auditors reviewed often did not contain sufficient guidance for individual units to develop additional procedures for implementing these policies, such as providing direction on IT standards and best practices that individual units should use. In addition, as previously mentioned, UA's university-wide IT security policies and procedures do not always fully align with IT standards and best practices. As a result, some UA individual units may not follow IT standards and best practices. For example, auditors reviewed two units' procedures for implementing the university-wide IT security policies in the five IT security control areas previously discussed and found that these units' procedures lacked several elements recommended by IT standards and best practices. Additionally, one of the units had not developed written procedures for two of the five areas. Therefore, when developing policies and procedures to address the recommendations in this finding, UA should either develop and implement university-wide procedures aligned with best practices that all individual units must follow or include sufficient guidance in its university-wide policies to help ensure its individual units develop procedures for implementing UA's policies that fully align with IT standards and best practices.

Recommendations

2.1. ASU should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

a. Developing and implementing additional written policies and procedures for its vulnerability management process that include requirements and/or guidance for:

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;
- Sharing scan results across the university to help eliminate similar vulnerabilities in other IT systems;
- Conducting penetration testing at specified frequencies based on risk;
- Using its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and
- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

b. Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing

baseline configurations, which provide a standard set of specifications for configuring all IT systems;

- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

c. Developing and implementing additional patch management policies and procedures to include guidance on how its staff should identify system flaws requiring patches and requirements for reporting those flaws to appropriate individuals for remediation.

d. Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Using secure coding standards when developing web applications;
- Requiring web application developers to be trained on developing secure software;
- Reviewing web application source code before web applications are released; and
- Performing security testing before web applications are released.

e. Developing and implementing policies and procedures for protecting system logs from unauthorized access, modification, and deletion.

f. Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

2.2. NAU should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

a. Finishing development of and implementing its draft policies and procedures establishing a vulnerability scanning process.

b. Developing and implementing additional written university-wide policies and procedures for penetration testing that include:

- Requirements for conducting penetration testing at specified frequencies based on risk.
- Guidance for its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and
- Guidance for helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all higher-risk web applications.

c. Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

d. Revising its configuration management policies and procedures to indicate that they apply to all NAU IT systems.

e. Finishing development of and implementing its draft patch management policies and procedures.

f. Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Gathering web application security requirements when developing web applications;
- Using secure coding standards when developing web applications;
- Requiring web application developers to be trained on developing secure software;
- Conducting threat modeling during web application development or security testing before releasing web applications to the live environment;
- Reviewing web application source code for web applications it develops internally before these web applications are released; and
- Performing security testing before web applications are released.

g. Developing and implementing written log monitoring policies and procedures that:

- Describe the critical IT systems and functions within each IT system that should be logged;
- Specify how frequently each log should be monitored;
- Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
- Require analysis of security-related information generated by log monitoring across the university to determine any patterns that might indicate a potential attack;
- Outline standard response actions for specific types of detected events, including informing designated personnel of security risks to the university and to individual IT systems; and
- Include requirements for securely protecting the logs, including protecting them from unauthorized access, modification, and deletion, and time frames for how long to retain the logs before deleting them.

h. Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and

- Correcting issues in a timely manner, including the development of corrective action plans, provision of training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

2.3. UA should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

a. Developing and implementing revised policies and procedures for its vulnerability management process that include requirements and/or guidance for:

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;
- Analyzing scan results, including specifying time frames for conducting the reviews, and sharing these results across the university to help eliminate similar vulnerabilities in other IT systems;
- Conducting penetration testing at specified frequencies based on risk;
- Using a risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and
- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

b. Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

c. Developing and implementing additional patch management policies and procedures that include the following:

- Identifying needed patches, reporting those patches to appropriate individuals responsible for remediation, and applying patches;
- Testing patches for effectiveness and potential side effects before installation; and
- Installing patches within required time frames.

d. Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Requiring web application developers to be trained on developing secure software;
- Reviewing web application source code before web applications are released; and

- Performing security testing before web applications are released.

e. Developing and implementing additional log monitoring policies and procedures that include the following requirements and guidance:

   - Specifying how frequently each log should be monitored;
   - Identifying who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
   - Analyzing security-related information generated by log monitoring across the university to determine any patterns that might indicate potential attack; and
   - Including requirements for securely protecting the logs and time frames for how long to retain the logs before deleting them.

f. Developing and implementing university-wide policies and procedures for:

   - Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
   - Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
   - Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

g. Developing and implementing university-wide procedures aligned with best practices that all individual units must follow when developing policies and procedures to address the recommendations in this finding; or include sufficient guidance in its university-wide policies to help ensure its individual units develop procedures for implementing UA's policies that fully align with IT standards and best practices.

ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

The State's universities—Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA)—have each established components of an information technology (IT) security governance framework, and NAU and UA should continue to revise, develop, and improve their framework components. IT security governance is the system by which an organization directs and controls IT security, and best practices recommend that an IT security governance framework include several components, such as an IT security strategic plan, documented roles and responsibilities, and policies and guidance. ASU has developed an IT security governance framework that is fully aligned with IT standards and best practices. NAU should continue efforts to align its IT security governance framework with best practices by revising its IT strategic plan to reflect organizational changes and by developing and implementing several policies and procedures. UA should fully align its IT security governance framework with best practices by developing and implementing an IT security strategic plan and several policies and procedures.

IT security governance foundational for establishing effective information security program

IT security governance is the system by which an organization directs and controls IT security and is foundational for establishing an effective information security program (see textbox for more information on information security programs). It provides an accountability and oversight framework that helps organizations ensure that IT security decisions are consistent with the organization's overall strategic direction, outlines an IT security decision-making process that includes organizational leaders and other stakeholders throughout an organization, and establishes a monitoring framework to help ensure that IT security objectives are achieved and that IT security risks are mitigated across an institution.[22] IT security standards and best practices published by EDUCAUSE and the National Institute of Standards and Technology (NIST) recommend that an IT security governance framework should include the following components:[23]

Information security program—An information security program is a documented approach for how an organization will select and implement appropriate IT security controls and demonstrate the effectiveness of satisfying its stated IT security requirements.

Source: Bowen, P., Hash, J., & Wilson, M. (2006). *NIST Special Publication 800-100: Information security handbook: A guide for managers*. Gaithersburg, MD: National Institute of Standards and Technology.

[22] Higher Education Information Security Guide. (n.d.) *Information security governance toolkit*. Retrieved from https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Governance.

[23] EDUCAUSE is a nonprofit association whose mission is to advance higher education through use of information technology. NIST is a federal agency within the United States Department of Commerce whose stated mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

- **IT security strategic plan—**Establishes institutional IT security initiatives and contains a mission, goals, and objectives aligned with the institution's overall strategic mission. Also, the strategic plan should include performance measures to assess progress toward achieving the IT security objectives.

- **Documented roles and responsibilities—**Describes how institutional leadership and stakeholders, such as business unit leaders, will be involved in and contribute to information security decisions, including responsibility for the creation, revision, oversight, and implementation of IT security controls (see textbox for more information on IT security controls).

- **Policies and guidance—**Describes how those charged with governance will guide management and protection of IT systems and the data contained in them and outlines the minimum information security controls that should be implemented across the institution, repercussions for policy noncompliance, and how policies and IT security controls should be communicated to those responsible for implementing them.

IT security controls—The safeguards or countermeasures designed to protect the confidentiality, integrity, and availability of IT systems and the data contained in them. Examples of security controls include security awareness training, antivirus software, and password policies specifying length and character requirements.

Source: National Institute of Standards and Technology (NIST). (2013). *NIST Special Publication 800-53, Revision 4: Security and privacy controls for federal systems and organizations*. Gaithersburg, MD.

- **Monitoring processes—**These processes assess the effectiveness of institutional information security practices and identify areas of policy noncompliance. Monitoring efforts should also inform revisions to information security practices and policies. One important component of monitoring is ensuring that third parties that obtain, use, or otherwise have access to an institution's data adequately secure this data.[24]

IT security governance can provide many benefits to an organization. For example, it establishes a foundation for effective risk management and a structure to optimize the allocation of information security resources. Additionally, IT security governance helps to ensure IT security decisions and practices are accepted and implemented consistently across an organization. Further, according to the Higher Education Information Security Council, IT security governance can help protect universities from reputational damage from IT security incidents while also strengthening stakeholder relationships.[25] Finally, according to EDUCAUSE, IT security governance is especially important in universities because they are generally large institutions with various colleges, departments, and other business units (units), often with diverse and unique IT and security needs.[26] Universities also maintain business, student, employee, donor, and research data in their IT systems and need to consider various laws and regulations that require certain data to be protected as they develop and implement IT security programs.

Each university has established IT security governance framework components, but NAU and UA should continue to improve their frameworks

Each university has established components of an IT security governance framework. Specifically, ASU has developed an IT security governance framework that is consistent with best practices and includes key components of an IT security governance framework. NAU has developed an IT security governance framework that includes three of the four recommended components, each of which is partially aligned with best practices; is in the process of revising its governance framework to reflect changes in its governance approach; and should continue efforts to further develop other components of and align its governance framework with IT standards and best practices. UA has developed an IT security governance framework with two of the four recommended components, and it should

[24] Third parties, such as vendors and other organizations, are any entities outside of an institution that have an agreement to access an institution's IT systems and/or access or store an institution's data.

[25] Higher Education Information Security Guide. (n.d.) *Information security governance toolkit*. Retrieved from https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Governance.

[26] Higher Education Information Security Council (HEISC) & EDUCAUSE Center for Analysis and Research (ECAR). (2016). *Technology in higher education: Information security leadership*. Louisville, CO: EDUCAUSE.

develop and implement additional policies and procedures to fully align its IT security governance framework with IT standards and best practices.

ASU has developed an IT security governance framework consistent with best practices— ASU has developed an IT security governance framework that is consistent with best practices and includes key components of an IT security governance framework (see textbox for a summary of ASU's governance framework). Specifically, ASU's IT security governance framework includes:

- **An IT security strategic plan that is consistent with best practices—**ASU has developed an IT security strategic plan that includes a mission, goals, and objectives that are consistent with ASU's overall strategic goals; plans for achieving its information security goals and objectives; and performance measures to assess progress on each objective. For example, ASU's IT security strategic plan contains an objective to improve incident response and threat detection, a performance measure to gauge progress toward this objective, and specific steps to improve incident response capabilities while enhancing threat detection.

ASU's governance framework includes all four recommended components—ASU has developed a governance framework that includes:

- An IT security strategic plan;
- Documented IT security roles and responsibilities;
- Policies and guidance documents; and
- Monitoring processes.

All four of ASU's IT security governance framework components are aligned with IT standards and best practices.

Source: Auditor General staff analysis of various documents provided by ASU.

- **Documented IT security roles and responsibilities that are consistent with best practices—**ASU has established and filled a chief information officer (CIO) position that has specific responsibilities related to IT security, including broad oversight of an information security office (ISO) and an information security program. Additionally, ASU has established and filled a chief information security officer (CISO) position that reports to the CIO. The CISO's primary responsibilities are to develop and maintain IT security policies, standards, and procedures; direct the day-to-day operations of ASU's ISO; and monitor the implementation and effectiveness of ASU's information security program. Further, ASU's individual units, such as academic colleges and departments, are responsible for implementing ASU's information security policies, standards, and procedures, although the ISO may assist the individual units if requested to do so. Ultimately, individual unit leaders, including college deans and department directors, are responsible for enforcing compliance with ASU's IT security policies, standards, and procedures. Although ASU's CIO and CISO do not have formal authority to enforce compliance with ASU's IT security policies, standards, and procedures, based on auditors' review of documentation, the ISO conducts monitoring to identify security incidents and advises individual units on potential remedies for these incidents, as needed. Finally, ASU has established several executive councils that include university leadership, ASU's CIO and CISO, and other university faculty and staff, to make decisions on IT security investments, such as cybersecurity tools to help monitor and assess security threats to ASU's network; to review university IT security monitoring results, risk assessments, data breaches involving other entities, and university incident response activities; and to discuss revisions to ASU's IT security policies.

- **Policies and guidance documents that are consistent with best practices—**ASU has established policies and guidance documents that outline IT security roles and responsibilities, security controls, appropriate and inappropriate IT activities, and repercussions for noncompliance with ASU's policies. Specifically, ASU has developed several policies and standards that provide IT security guidance to the users of ASU's IT resources. For example, ASU has developed an IT security policy based on federal and state laws and regulations that establishes university-wide guidelines and standards for protecting the confidentiality, integrity, and availability of ASU's IT resources. ASU has also developed a policy that defines acceptable uses of ASU's computing and communication resources. Finally, ASU has developed an information security program that describes how it will guide the management and protection of its IT systems and the data contained in them, including outlining its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls.

- **Processes for monitoring the effectiveness of its IT security practices, identifying policy noncompliance, monitoring third parties, and identifying the need for IT security changes—**ASU has developed processes to monitor the effectiveness of institutional IT security practices, and to identify policy noncompliance and information security program revisions. For example, ASU tracks various IT security measures and metrics, such as the number of unauthorized attempts to access its network and the number of systems without current antivirus software. ASU's executive councils use information from this monitoring to make decisions, such as determining the need for new IT security investments. Additionally, because ASU's individual units are responsible for implementing its information security program, ASU's ISO develops performance reports for each ASU unit focusing on specific security measures and outlining potential risks, such as the number of faculty and staff who have completed annual security training and the number of systems without installed or updated anti-virus software, and the ISO shares these performance reports with its individual units. The individual units are then responsible for addressing any issues identified in the performance reports. ASU also requires third parties that have access to ASU's sensitive data to conduct security assessments of their processes for protecting data and to provide assessment results to ASU.[27] Further, if a third party is directly hosting, receiving, storing, or analyzing ASU's data, ASU requires the third party to contract for and provide ASU with the results of an external audit of its IT security controls.

NAU has developed an IT security governance framework that is partially aligned with best practices and should continue to develop and revise key framework components—NAU has developed an IT security governance framework that includes three of the four recommended components, one of which is fully aligned and two of which are partially aligned with best practices (see textbox for a summary of NAU's governance framework). Specifically, NAU has:

- **An IT security strategic plan but is revising this strategic plan to reflect changes in its IT security governance approach and align the plan with its overall strategic goals—**NAU has an IT security strategic plan that includes a mission, goals, and objectives; plans for achieving its information security goals and objectives; and performance measures to assess progress on each objective. However, consistent with IT standards and best practices, NAU reported that it is revising its IT security strategic plan to reflect changes in its governance approach for IT security and to further align it with NAU's overall strategic goals.[28] Specifically, beginning in 2016, in an effort to increase the efficiency of its IT security operations, NAU began to transition from a decentralized IT security governance approach, where most of its IT security staff and operations were housed in its individual units, such as academic colleges and departments and other business units, to a more centralized approach, where most of its IT security staff and operations are housed in NAU's Information Technology

NAU's governance framework includes three of the four recommended components—NAU has developed a governance framework partially aligned with best practices that includes:

- An IT security strategic plan that includes the elements recommended by best practices. However, NAU is revising the IT security strategic plan to reflect changes in its governance approach and to align the plan with its overall strategic goals;
- Documented IT security roles and responsibilities that are aligned with best practices; and
- Policies and guidance documents that include some elements recommended by best practices but are being further developed to more fully align with best practices and to reflect changes in its governance approach.

NAU does not have policies and procedures establishing monitoring processes that are consistent with IT standards and best practices but reported that it plans to develop these policies and procedures once it has finished revising and developing its other IT security governance framework components.

Source: Auditor General staff analysis of various documents provided by NAU and interviews with NAU staff.

[27] As discussed in the Introduction (see page 1), the universities use IT systems to store and process various types of sensitive data, including names, birthdates, and social security numbers, as well as financial and health information and educational records.

[28] According to EDUCAUSE, organizations should revise their IT security governance frameworks to reflect any changes in their IT security governance structures and practices. See HEISC & ECAR, 2016.

Services (ITS) department.[29] In addition, NAU reported that it is in the process of revising its university-wide strategic plan. As a result, as of February 2018, NAU had begun to develop a new IT security strategic plan to reflect its new governance approach and to align it with revisions NAU makes to its university-wide strategic plan. NAU estimated it will complete its new IT security strategic plan by fall 2018.

- **Documented IT security roles and responsibilities that are consistent with best practices—**NAU has documented IT security governance roles and responsibilities in various university policies and charters. Specifically, NAU has a CIO who is responsible for overseeing NAU's IT security program, among other duties, including overseeing NAU's ITS department. Additionally, NAU has a Director of Information Security who reports to the CIO and is responsible for developing and implementing IT security policies, standards, and procedures and overseeing the operations of NAU's ISO, which is a component unit of NAU's ITS department. NAU's ITS department is responsible for implementing NAU's IT security policies, standards, and procedures for most of NAU's units, and ten individual unit leaders, including college deans and department directors, have this responsibility for their units. NAU's ITS department is also responsible for enforcing compliance with NAU's information security policies, standards, and procedures university-wide. NAU's ISO monitors some information security measures, such as the number of attempts by hackers to obtain sensitive data, including usernames, passwords, and credit card information. Finally, NAU has established several executive councils that include university leadership, NAU's CIO and Director of Information Security, and other university faculty and staff who make decisions on the allocation of IT security resources, review IT security concerns and issues, and discuss revisions to IT security policies.

- **Established policies and guidance that include some, but not all, best practice elements—**NAU has developed policies and guidance documents that outline IT security roles and responsibilities, some IT security controls, appropriate and inappropriate IT activities, and repercussions for noncompliance with NAU's policies. For example, NAU has developed a policy that defines the appropriate use of its IT resources, including specifying repercussions for violating the policy. In addition, it has established policies outlining some IT security controls, such as procedures for how NAU staff should respond to IT security incidents (see Finding 4, pages 42 through 44, for more information on incident response).

  Although NAU's policies and guidance include some best practice elements, they are not fully aligned with IT standards and best practices or its current governance approach. Specifically, as discussed in Finding 4 (see pages 37 through 45), NAU needs to take steps to develop, revise, and implement policies and procedures in three key IT security areas. Similarly, an October 2017 Office of the Auditor General report that assessed NAU's internal controls over financial reporting found that NAU did not have sufficient written IT security policies and procedures in several areas recommended by IT standards and best practices.[30] As of April 2018, NAU had developed several draft IT security policies to help address these deficient areas, including an information security policy outlining the minimum set of IT security controls that should be implemented university-wide, such as data classification and incident response processes. In addition, as of January 2018, to reflect the changes in its governance approach, NAU had begun developing a draft information security program that describes how it will guide the management and protection of its IT systems and the data contained in them, including outlining its overall approach for selecting, implementing, and assessing its IT security controls' effectiveness.

- **Not developed formal processes for monitoring the effectiveness of its IT security practices, identifying policy noncompliance, monitoring third parties, or identifying the need for IT security changes—**NAU monitors several IT security measures such as the number of hacking attempts to obtain sensitive data, including usernames, passwords, and credit card information. However, NAU has not developed policies and procedures establishing monitoring processes to assess the effectiveness of its IT security practices, to identify policy noncompliance, to monitor and assess third parties' compliance with contract or agreement requirements related to IT security, or to identify the need for changes to its IT security

[29] NAU has transitioned IT security staff to its ITS department in phases based on factors such as the complexity of units' IT operations and the potential for staff turnover. As of April 2018, 10 of NAU's 224 reported individual units retained their own IT staff and operations.

[30] See Auditor General report *Northern Arizona University: Report on internal control and compliance, year ended June 30, 2017*.

practices based on monitoring results. As of April 2018, NAU had drafted a policy to monitor some IT activities such as the use of passwords. NAU reported that it plans to develop additional monitoring processes once it has finished developing its other governance framework components.

To help ensure it provides effective IT security governance, NAU should continue its efforts to fully align its IT security governance framework with IT standards and best practices by:

- Finishing developing and implementing its draft IT security strategic plan, including developing a mission, goals, and objectives aligned with NAU's overall strategic mission, and performance measures to assess progress toward achieving those objectives;
- Finishing developing and implementing its draft information security policy and draft information security program including outlining how its policies and IT security controls should be communicated to those responsible for implementing them; and
- Developing and implementing policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

Finally, NAU should develop and implement policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security. According to EDUCAUSE, this monitoring can be risk based.[31] For example, NAU could assess the risk of third-party contractors based on risk factors such as whether they are hosting, receiving, storing, or analyzing data that NAU determines to be sensitive and/or mission critical and require higher-risk contractors to provide NAU with the results of an external audit of their IT security controls.

UA has developed an IT security governance framework but should continue to develop and revise key framework components—UA has developed an IT security governance framework with two of the four recommended components, one of which is fully aligned with best practices, but has not developed the other two recommended components (see textbox for a summary of UA's governance framework). Specifically, UA has:

- **Not developed an IT security strategic plan—**Although UA has developed a document that outlines several strategic initiatives for IT security, UA has yet to develop an IT security strategic plan that contains a mission, goals, and objectives that are aligned with the UA's overall strategic mission and that includes performance measures to assess progress toward achieving those objectives.
- **Documented roles and responsibilities that are consistent with best practices—**UA has documented IT security governance roles and responsibilities in various university policies and committee charters. For example, UA has established a Vice President for Information

UA's governance framework includes two of the four recommended components—UA has developed a governance framework partially aligned with best practices that includes:

- Documented IT security roles and responsibilities that are aligned with best practices; and
- Policies and guidance documents that include some elements recommended by best practices, but that lack other elements and do not always reflect UA's current IT security practices.

Although UA has developed a document that outlines several strategic initiatives for IT security, it does not include the elements of an IT security strategic plan recommended by best practices. Additionally, UA does not have policies and procedures establishing monitoring processes that are consistent with IT standards and best practices.

In fiscal year 2018, UA began hiring several new IT security staff and reported that it has begun the process of aligning its IT security governance framework with IT standards and best practices.

Source: Auditor General staff analysis of various documents provided by UA and interviews with UA staff.

[31] Higher Education Information Security Guide. (n.d.) *Vendor and third-party management*. Retrieved from https://spaces.internet2.edu/display/2014infosecurityguide/Vendor+and+Third-Party+Management.

Strategy and University Libraries (VPISUL) who oversees UA's information security program and IT security of the IT systems related to UA's core functions, such as its financial system. As of April 2018, UA hired a CIO who reports to the VPISUL and is responsible for developing an IT security strategic plan and directing the day-to-day operations of UA's University Information Technology Services (UITS) office. Additionally, UA has a CISO who reports to the CIO and is responsible for developing and enforcing UA's IT security policies, standards, and procedures and directing the day-to-day operations of UA's ISO, which is a component unit of UA's UITS office. All of UA's units, such as academic colleges and departments and other business units, are responsible for implementing and ensuring compliance with UA's IT security policies, standards, and procedures in their units. UA has also established several executive councils and committees that include UA leadership, UA's VPISUL, CIO, and CISO, and other university faculty and staff. These councils and committees work with the VPISUL, CIO, and CISO in several areas, including the allocation of IT security resources, discussing IT security concerns and issues, and identifying revisions to IT security policies.

- **Established policies and guidance that include some best practice elements but lack other elements—**UA has developed policies and guidance for IT security that outline roles and responsibilities, establish the minimum IT security controls that should be implemented across the university, and set repercussions for policy noncompliance. For example, UA has established an IT security policy that requires each individual unit to protect UA's resources by adopting and implementing, at a minimum, the security standards and procedures the CISO developed, and that policy violations may result in consequences such as losing data access privileges. However, as discussed in Finding 2 (see page 22), although UA has developed university-wide IT security policies and procedures, these policies and procedures often did not contain sufficient guidance for individual units to develop additional procedures for implementing these policies, such as providing direction on IT standards and best practices that individual units should use. Further, UA has not developed a policy or guidance document explaining how it will guide the management and protection of its IT systems and the data contained in them, such as an information security program that outlines its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls and explains how it will communicate UA's policies and IT security controls to those responsible for implementing them.

- **Not developed processes for monitoring the effectiveness of its IT security practices, identifying policy noncompliance, monitoring third parties, or identifying the need for IT security changes—**As of March 2018, UA had yet to develop policies and procedures establishing monitoring processes to assess the effectiveness of its IT security practices, to identify policy noncompliance, to monitor and assess third parties' compliance with contract or agreement requirements related to IT security, or to identify the need for changes to its IT security practices based on monitoring results. Similarly, an October 2017 Office of the Auditor General report that assessed internal controls over financial reporting found that UA did not conduct monitoring to ensure its IT security policies and procedures were established and followed university-wide.[32] In response to the October 2017 report, UA indicated that it planned to install network monitoring tools to allow UA staff to conduct monitoring and oversight of its IT security practices. As of February 2018, a UA official reported that UA was in the early stages of installing and testing these network monitoring tools.

According to UA, lack of staff resources and vacancies in key positions have contributed to the deficiencies in some of the components of its IT security governance framework, but it has taken some steps to address these issues. Specifically, prior to fiscal year 2018, UA's ISO had two employees, including its CISO, and these two employees had other job responsibilities beyond developing and enforcing UA's IT security policies, standards, and procedures. For example, these two employees had responsibility for implementing IT security controls for UA's IT systems related to its core functions, such as its financial system. In addition, prior to hiring a new CIO in April 2018, UA's VPISUL was responsible for the CIO's duties in addition to the VPISUL's duties. However, as of January 2018, UA's ISO reported that it had hired five new employees and, as of March 2018, had been authorized to hire five additional employees. According to UA, adding its CIO and several new ISO staff will allow it to fully align its IT security governance framework with IT standards and best practices.

[32] See Auditor General report *University of Arizona: Report on internal control and compliance, year ended June 30, 2017*.

Therefore, UA should fully align its IT security governance framework with IT standards and best practices by developing and implementing:

- An IT security strategic plan that contains a mission, goals, and objectives aligned with UA's overall strategic mission and includes performance measures to assess progress toward achieving those objectives.
- IT security policies and guidance documents that explain how UA will guide the management and protection of its IT systems and the data contained in them, such as developing an information security program that outlines its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls and explains how it will communicate UA's policies and IT security controls to those responsible for implementing them; and
- Policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

Finally, UA should develop and implement policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security. As previously mentioned, according to EDUCAUSE, this monitoring could be risk based. For example, UA could assess the risk of third-party contractors based on risk factors such as whether they are hosting, receiving, storing, or analyzing data that UA determines to be sensitive and/or mission critical and require higher-risk contractors to provide UA with the results of an external audit of their IT security controls.

Recommendations

3.1. NAU should:

a. Finish developing and implement its draft IT security strategic plan including developing a mission, goals, and objectives aligned with NAU's overall strategic mission, and performance measures to assess progress toward achieving those objectives.

b. Finish developing and implement its draft information security policy and draft information security program, including outlining how its policies and IT security controls should be communicated to those responsible for implementing them.

c. Develop and implement policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

d. Develop and implement policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security.

3.2. UA should develop and implement:

a. An IT security strategic plan that contains a mission, goals, and objectives aligned with UA's overall strategic mission and includes performance measures to assess progress toward achieving those objectives.

b. IT security policies and guidance documents that explain how UA will guide the management and protection of its IT systems and the data contained in them, such as developing an information security program that outlines its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls and explains how it will communicate UA's policies and IT security controls to those responsible for implementing them.

c. Policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

d. Policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security.

Universities should improve processes in three key information security program areas

Although Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA) have either wholly or partially implemented appropriate data classification, risk assessment, and incident response processes, which are important for adequately protecting their information technology (IT) systems and the data contained in them, including sensitive data, each university should take steps to improve in one or more of these areas.[33] Specifically:

- ASU, NAU, and UA have each established elements of a data classification process, which is important for ensuring that sensitive data, such as confidential information, is protected from loss, misuse, or disclosure. However, ASU and UA should develop and implement policies and procedures requiring the development of data inventories to help ensure their data is appropriately and consistently classified and protected. NAU should revise its data classification policies and procedures to include a requirement to periodically review and update the classification of its data to ensure the data is appropriately classified, and it should take steps to ensure its data classification policies and procedures are implemented university-wide.

- ASU has developed and implemented an appropriate IT risk assessment process, which is important for adequately protecting sensitive data or critical IT systems by identifying and reducing security threats, such as computer-assisted fraud. However, NAU has not conducted an IT risk assessment, should revise its IT risk assessment policy to include a requirement to report risk assessment results to NAU leadership, assign responsibility for conducting IT risk assessments, and develop and implement procedures for conducting an IT risk assessment. UA should revise its IT risk assessment policies and procedures to include a requirement to address identified risks, and it should fully implement its IT risk assessment process.

- Finally, ASU, NAU, and UA have each developed an incident response process, which is important for reducing and minimizing the impact of IT security incidents, such as a breach involving confidential information, and ASU's process aligns with IT standards and best practices. However, NAU and UA should improve their incident response processes by developing and implementing policies and procedures for training incident response personnel and for testing their incident response processes, and UA should develop procedures for assessing staff compliance with its incident response policies and procedures.

ASU and UA should further align their data classification processes with best practices, and NAU should implement its data classification process university-wide

Data classification is a process that helps to ensure sensitive data, such as confidential information, is protected from loss, misuse, or inappropriate disclosure. Specifically, a data classification process identifies whether data is sensitive and stipulates how it should be protected based on the data's inherent level of risk, considering criteria such as whether the data is public or confidential. According to IT standards and best practices, a data classification process is critical to help ensure that sensitive data is identified, inventoried, and then protected based on risk, as

[33] As discussed in the Introduction (see page 1), the universities use IT systems to store and process various types of sensitive data, including names, birthdates, social security numbers, financial and health information, and educational records.

well as to prevent unauthorized data access, modification, disclosure, and destruction. Additionally, appropriately classifying data helps organizations determine which IT systems hold the most sensitive and high-risk data, which facilitates other important processes, including IT risk assessments, vulnerability management, and secure web application development (see pages 40 through 42 for more information on IT risk assessments; Finding 2, pages 13 through 16, for additional information on vulnerability management; and Finding 2, pages 18 through 19, for additional information on web application development). Further, data classification helps to ensure that organizations meet statutory and regulatory requirements such as those regarding the privacy of student information and certain health information.[34] IT standards and best practices indicate that data classification should include an organization-wide data classification process (see textbox for IT standards and best practices for data classification).

Although each university has established data classification policies and procedures that are generally consistent with best practices, ASU's data classification policies and procedures do not include a requirement for its individual colleges, departments, and other business units (units) to develop a data inventory, NAU has not yet implemented its data classification policies and procedures, and UA's data classification policy also does not include a requirement for individual units to develop a data inventory. Specifically:

- **ASU's data classification process partially aligns with best practices, but it should require each individual unit to develop a data inventory, and develop and implement a plan to ensure these data inventories are completed—**ASU has developed policies and procedures for a data classification process that partially align with IT standards and best practices.[35] These data classification policies and procedures apply to all university-managed data, and describe four different levels of data classification based on risk, such as public or highly sensitive, and the type of data included in each classification level is related to the potential risks of the loss or misuse of this data. For example, ASU's highly sensitive classification level includes data on human health, life, and safety matters because of the potential risk associated with the unauthorized use or disclosure of this type of information. Additionally, the policies and procedures specify that additional controls should be implemented based on the risks associated with each data classification level, such as by using encryption to protect highly sensitive data.

  However, ASU's data classification policies and procedures do not include some best practice components that are important for ensuring its data is consistently and appropriately classified. Specifically, ASU's data classification policies and procedures do not include a requirement for each individual unit to develop a data inventory for its IT systems as part of its data classification process or to periodically review its classification

Data classification process criteria

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

- Classifies data with similar protection needs based on requirements such as confidentiality and legal or regulatory requirements and specifies information security procedures that apply to all the information in each class;
- Consists of an inventory of data classification details (data inventory) for IT systems that includes the data's classification level, identity of the data owner, and a brief description of the data classified; and
- Includes a requirement to periodically review classification of data to ensure that the data is appropriately classified and to update the data inventory as necessary.

Source: Auditor General staff analysis of IT standards and best practices: International Organization for Standardization. (2013). *Code of practice for information security controls*, ISO/IEC 27002. Geneva, Switzerland; and National Institute of Standards and Technology (NIST). (2013). *NIST Special Publication 800-53, Revision 4: Security and privacy controls for federal systems and organizations*. Gaithersburg, MD.

[34] The Family Educational Rights and Privacy Act (FERPA) requires the universities to keep student records private. In addition, certain health-specific information, which some universities maintain, is subject to notification requirements under the federal Health Insurance Portability and Accountability Act (HIPAA) (see Introduction, page 1, for additional information on FERPA requirements and page 2 for additional information on HIPAA requirements).

[35] The terminology "policies and procedures" collectively refer to various IT security guidance documents that the universities may classify as standards, policies, procedures, plans, and/or guidelines.

of data to determine the need for updating its data inventory. As a result, ASU's individual units may not be documenting their data classification results or may not be doing so consistently across all units. Additionally, ASU's individual units may not consistently or appropriately identify and address changes in their data, such as newly acquired sensitive data that a unit did not previously maintain in its IT systems, that could require reclassifying the data and/or implementing additional controls to adequately protect the data. Further, without data inventories, those ASU staff who are responsible for overseeing IT security may lack the information necessary to determine if all individual units have appropriately and consistently classified and protected their data. Finally, having an inventory of its IT systems would help ASU implement the recommendation previously discussed in Finding 2 (see page 14) for regularly scanning all the IT systems on its network and its web applications based on risk factors such as the amount and nature of sensitive data contained in these IT systems and web applications.

Therefore, ASU should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified, and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified. In addition, ASU should establish time frames and guidance for regularly reviewing and updating data inventories. Further, ASU should develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

- **NAU's data classification process partially aligns with best practices, but it should periodically review and update its data classification and develop a plan for implementing its data classification process—**As of February 2018, NAU had developed policies and procedures for a new data classification process that partially align with IT standards and best practices. These policies and procedures apply to all university information and describe four levels of data classification based on risk level, such as public or highly sensitive, and the type of data included in each classification level is related to the potential risks of the loss or misuse of this information, similar to ASU. Additionally, NAU's data classification policies and procedures specify controls that should be implemented based on the risks associated with each data classification level, such as using encryption to protect highly sensitive data. Finally, NAU's policies and procedures require the classification of all data and the development of a data inventory that includes the data's classification level, a brief description of the data, and the data owner's identity.

  However, NAU's data classification policies and procedures do not include a requirement for each of its individual units to periodically review its classification of data to ensure the data is appropriately classified and to determine the need for updating its data inventory. Therefore, NAU should revise its data classification policies and procedures to include a requirement for each individual unit to periodically review its classification of data to ensure the data is appropriately classified and to update its data inventory as necessary. In addition, as of March 2018, NAU had not implemented its data classification policies and procedures and should develop a plan for doing so, including establishing a deadline by which all individual units must complete the data classification process and develop data inventories, and following up with individual units to ensure they have completed the process.

- **UA's data classification process partially aligns with best practices, but it should require each individual unit to develop a data inventory and develop and implement a plan to ensure these data inventories are completed—**UA has developed data classification policies and procedures that partially align with IT standards and best practices. These policies and procedures apply to all university data and describe four levels of data classification based on risk level, such as public or regulated, and the type of information included in each classification level is related to the potential risks of the loss or misuse of this information, similar to ASU and NAU. Additionally, UA's data classification policies and procedures specify controls that should be implemented based on the risks associated with each data classification level, such as using encryption to protect regulated data.

  However, UA's data classification policies and procedures do not include a requirement for each of its individual units to develop a data inventory or to periodically review its classification of data to ensure the

data is appropriately classified and to determine the need for updating its data inventory. Having a data inventory of its IT systems would help UA implement the recommendation previously discussed in Finding 2 (see pages 15 through 16) for regularly scanning all the IT systems on its network and its web applications based on risk factors such as the amount and nature of sensitive data contained in these IT systems and web applications. Therefore, similar to ASU, UA should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified, and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified. In addition, it should establish time frames and guidance for regularly reviewing and updating data inventories. Further, UA should develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all units must complete a data inventory and follow-up procedures to ensure all units have done so.

ASU has implemented an appropriate IT risk assessment process, but NAU and UA should improve their IT risk assessment processes and implement them university-wide

An IT risk assessment is a structured process that is used to identify, estimate, and prioritize risks to an organization's operations that result from the use of IT systems. According to IT standards and best practices, IT risk assessments are used to manage risk, either by implementing controls to mitigate risk or by accepting risk. Without an effective IT risk assessment process, organizations may not be able to adequately protect sensitive data or critical IT systems by addressing security threats, such as computer-assisted fraud, vandalism, and fire or flood. IT standards and best practices state that organizations should develop an organization-wide IT risk assessment process (see textbox for IT standards and best practices for IT risk assessment).

ASU has developed appropriate IT risk assessment policies and procedures that have been implemented university-wide. However, NAU has not implemented its IT risk assessment policy or conducted an IT risk assessment, and although UA's IT risk assessment policies and procedures align with best practices, it has not fully implemented these policies and procedures. Specifically:

- **ASU's IT risk assessment process aligns with best practices and has been implemented university-wide—**ASU has developed policies and procedures for an IT risk assessment process that are consistent with IT standards and best practices. Specifically, its policies and procedures specify the process for conducting an IT risk assessment, including assigning roles and responsibilities, and indicate that IT risk assessments will be conducted regularly. In addition, ASU's policies and procedures outline a structured methodology for assessing risks to IT systems and data, including identifying both internal and external vulnerabilities. Finally, ASU's policies and procedures include a requirement to document IT risk assessment results, develop corrective actions that address the highest-priority risks university-wide, and share the results with ASU's leadership.

IT risk assessment process criteria

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

- Assigns roles and responsibility for the IT risk assessment process;
- Requires regular assessments;
- Consists of a structured methodology for assessing risks, including identifying both internal and external vulnerabilities;
- Documents results and potential impacts of risks;
- Uses results to help manage and address risks, such as by implementing controls to protect against identified risks; and
- Reports results to organizational leadership.

Source: Auditor General staff analysis of IT standards and best practices: National Institute of Standards and Technology (NIST). (2012). *NIST Special Publication 800-30, Revision 1: Guide for conducting risk assessments*. Gaithersburg, MD.; International Organization for Standardization, 2013; and NIST, 2013.

ASU has implemented its IT risk assessment process across the university. Specifically, in 2017, all of ASU's individual units, such as academic colleges and departments, completed an IT risk assessment. Based

on the IT risk assessment results, ASU identified four university-wide, high-risk focus areas and developed recommendations for its individual units to implement to address these areas, as necessary. For example, one of the four high-risk focus areas was security awareness, and ASU recommended that individual unit staff address deficiencies in this area by taking various actions, such as using standard letters to remind faculty and staff to complete required security awareness training. ASU's information security office (ISO) staff reported that they will continue conducting IT risk assessments in both 2018 and 2019 to evaluate individual unit progress toward implementing recommendations in the four high-risk focus areas and to also identify new risks.

- **NAU's IT risk assessment process partially aligns with best practices, but it has not conducted an IT risk assessment and should improve its IT risk assessment policies and procedures—**NAU has an IT risk assessment policy dated May 2009, which is partially aligned with IT standards and best practices. This policy outlines some roles and responsibilities for the IT risk assessment process, such as assigning staff to develop procedures and guidelines for implementing the policy. In addition, the policy includes a requirement to periodically conduct university-wide IT risk assessments using a systematic approach to determine the significance of risk and use the results to implement controls to protect against identified risks.

  However, as of March 2018, NAU had not developed IT risk assessment procedures and guidelines for conducting IT risk assessments. The IT risk assessment policy also does not assign roles and responsibilities for conducting IT risk assessments. As a result, NAU was unable to provide evidence that it had ever conducted a university-wide IT risk assessment. In addition, NAU's IT risk assessment policy does not include a requirement to report the results of its IT risk assessment to NAU leadership. Therefore, to help ensure it regularly conducts IT risk assessments and takes appropriate actions to address the results of these assessments, NAU should develop and implement university-wide IT risk assessment policies and procedures for conducting IT risk assessments; compiling and evaluating the results; using the results to manage and address identified risks, such as by implementing controls to protect against identified risks; and reporting the results to NAU's leadership. Additionally, the policies and procedures should assign roles and responsibilities for conducting and completing these various requirements and procedures.

- **UA's IT risk assessment process partially aligns with best practices, but its policies and procedures should require using risk assessment results to address identified risks, and it should fully implement its process—**UA has developed IT risk assessment policies and procedures that are consistent with IT standards and best practices. Specifically, these policies and procedures include a requirement for all of UA's individual units to regularly complete an IT risk assessment; describe the process to complete the IT risk assessment, including assigning roles and responsibilities; and require the results to be formally documented and analyzed to determine a university-wide IT risk profile. Finally, UA's policies and procedures direct its ISO staff to report the results of the IT risk assessment to UA leadership.

  However, UA's IT risk assessment policies and procedures recommend but do not require its individual units to use IT risk assessment results to address identified risks, and it has not fully implemented its IT risk assessment process. Specifically, although UA's policies and procedures include a requirement to formally document the IT risk assessment results, and indicate that individual units can use the results from their IT risk assessments to measure risk and identify controls, its policies and procedures do not require individual units to use the results to manage and address identified risks. In addition, UA conducted its most recent IT risk assessment in 2016, but UA staff reported that approximately 17 percent of its individual units did not complete the IT risk assessment. Further, although its policies and procedures require UA to analyze and formally document the results of its IT risk assessment, UA's ISO staff reported they did not have the resources to do so, and as a result, UA did not develop a university-wide IT risk profile. UA's ISO staff also reported that they plan to conduct an IT risk assessment using the same procedure in 2018 and that they intend to develop the capacity to compile and analyze results to establish a university-wide IT risk profile that will be communicated to UA's leadership. Therefore, UA should revise its IT risk assessment policies and procedures to include a requirement for managing and addressing identified risks, such as by implementing controls to protect against identified risks. In addition, it should fully implement its IT risk assessment process by conducting the IT risk assessment in all UA individual units, compiling and analyzing the results of the

IT risk assessment, using these results to establish a university-wide IT risk profile, and communicating the results to UA's leadership.

ASU has implemented an appropriate incident response process, but NAU and UA should improve their incident response processes and implement them university-wide

Incident response is the process of detecting, reporting, and responding to information security incidents, such as a breach involving confidential information. IT standards and best practices indicate that effective incident response reduces the risk of these incidents occurring, minimizes their overall impact, and ensures that legal requirements are followed if a security breach occurs (see textbox for IT standards and best practices for incident response). For example, Arizona Revised Statutes (A.R.S.) §18-545 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.[36]

Incident response process criteria

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

- Defines IT security incident and related terms;
- Identifies roles and responsibilities for the incident response process;
- 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; and
- Includes incident response training, testing, and monitoring.

Source: Auditor General staff analysis of IT standards and best practices: Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *NIST Special Publication 800-61, Revision 2: Computer security incident handling guide*. Gaithersburg, MD: National Institute of Standards and Technology; and NIST, 2013.

ASU, NAU, and UA have each established an incident response process. Although ASU's process is consistent with best practices, NAU and UA should take steps to improve their incident response processes. Specifically:

- **ASU has developed and implemented an incident response process that aligns with best practices—**ASU has developed incident response policies and procedures that are consistent with IT standards and best practices. Specifically, these policies and procedures apply to all of ASU's individual units, define an information security incident, and include details for identifying, responding to, recovering from, and following up on information security incidents. Additionally, ASU's policies and procedures assign roles and responsibilities for implementing its incident response process, which incorporate the designated authority to make decisions as appropriate, and include requirements for incident response training, testing, and monitoring. ASU has also developed guidance documents for ASU's IT staff to use when responding to several different types of incidents, such as an email phishing attack (see Finding 1, page 6, for additional information about email phishing). These guidance documents list steps for handling specific types of incidents and include processes for revising these steps as necessary based on lessons learned after each incident.

  Auditors reviewed ASU's response to an incident and found that ASU staff followed its incident response policies and procedures. Specifically, auditors reviewed ASU's documentation outlining how its staff responded to a specific email phishing incident and found that ASU's IT staff followed its incident response policies and procedures for appropriately responding to the incident, including documenting the specific steps taken to investigate, respond to, recover from, and follow up on the incident.

[36] A.R.S. §18-545 does not apply to financial institutions obligated to protect nonpublic personal information of its customers per Title V of the federal Gramm-Leach-Bliley Act, covered entities as defined under HIPAA, the Arizona Department of Public Safety, county sheriffs' departments, municipal police departments, prosecution agencies, or courts because these entities must follow other notification procedures outlined in federal and state laws.

- **NAU is enhancing its incident response process to further align it with best practices—**NAU has developed policies and procedures for an incident response process that are partially aligned with IT standards and best practices. Specifically, these policies and procedures apply to all NAU's individual units, define an incident, outline incident response roles and responsibilities, and provide decision-making authority to individuals responsible for implementing NAU's incident response process. Its policies and procedures also include steps that provide guidance for reporting, identifying, responding to, recovering from, and following up on security incidents. Finally, NAU's incident response policies and procedures indicate that it will track incidents to monitor its incident response process.

  However, NAU's incident response process does not fully align with IT standards and best practices. Specifically, NAU's incident response policies and procedures do not include information about training or testing related to its incident response process. As of February 2018, NAU's Information Technology Services (ITS) department staff convened an incident response and incident management project group that began revising its incident response process, including reviewing another university's incident response handbook as a reference for potential practices that NAU could adopt to help fully align its process with IT standards and best practices. NAU's ITS department staff estimated they will complete revisions to NAU's incident response policies and procedures to fully align the incident response process with IT standards and best practices by August 2018. NAU should continue its efforts to further align its incident response process with IT standards and best practices and ensure its incident response policies and procedures address training for incident response personnel and testing its incident response process, including establishing time frames for training and testing.

- **UA should further align its incident response process with IT standards and best practices and ensure staff compliance with its incident response policies and procedures—**UA has developed policies and procedures for an incident response process that are partially aligned with best practices. Specifically, these policies and procedures define information security incident terms, include incident response roles and responsibilities, and provide decision-making authority to individuals responsible for implementing UA's incident response process. In addition, UA has developed incident response procedures that detail how individual unit IT staff should detect, analyze, report, contain, eradicate, and recover from a security incident. Further, UA's incident response policies and procedures indicate that when any UA computer user believes an incident has occurred, the user should report the incident to individual unit IT personnel and that these personnel should report serious incidents to UA's ISO.[37] Finally, UA's incident response policies and procedures indicate that it will track incidents to monitor its incident response process.

  However, UA's incident response process does not fully align with IT standards and best practices. Specifically, UA's policies and procedures do not include information about training or testing related to its incident response process. Therefore, UA should develop and implement incident response policies and procedures for training incident response personnel and for testing its incident response process, including establishing time frames for training and testing.

  Additionally, UA has not always followed its incident response process. Specifically, auditors reviewed UA's documentation of its response to a series of incidents that potentially allowed unauthorized access to UA's IT systems over a span of approximately 5 years and found that UA staff did not follow its incident response policies and procedures. For example, although UA's incident response policies and procedures require the investigation of an incident to be documented, including describing the containment, eradication, and recovery from incidents, UA was not able to provide documentation that reflected the specific steps it took to contain and recover from these incidents. As previously discussed in Finding 3 (see page 34), UA needs to develop and implement policies and procedures establishing a monitoring process to identify areas of policy noncompliance. UA should also develop procedures for assessing whether UA staff are complying with its

[37] UA defines a serious incident as attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy, including UA's university-wide policy for acceptable use of computers and networks, that may pose a threat to UA's resources, stakeholders, and/or services. Additionally, a serious incident must meet one or more other specified criteria, such as involving serious legal issues or causing severe disruption to critical services.

incident response policies and procedures and, as recommended in Finding 2 (see pages 20 through 22), take steps to help ensure identified instances of noncompliance are adequately addressed.

Recommendations

4.1. ASU should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified.

4.2. ASU should:

a. Establish time frames and guidance for regularly reviewing and updating data inventories; and

b. Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

4.3. NAU should revise its data classification policies and procedures to include a requirement to periodically review its classification of data to ensure the data is appropriately classified and to update its data inventory, as necessary.

4.4. NAU should develop a plan for implementing its data classification policies and procedures, including:

a. Establishing a deadline by which all individual units must complete the data classification process and develop data inventories; and

b. Following up with individual units to ensure they have completed the process.

4.5. UA should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified, and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified.

4.6. UA should:

a. Establish time frames and guidance for regularly reviewing and updating data inventories; and

b. Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

4.7. NAU should develop and implement university-wide IT risk assessment policies and procedures for conducting IT risk assessments, compiling and evaluating the results, using the results to manage and address identified risks, such as by implementing controls to protect against identified risks, and reporting the results to NAU's leadership. Additionally, the policies and procedures should assign roles and responsibilities for conducting and completing these various requirements and procedures.

4.8. UA should revise its IT risk assessment policies and procedures to include a requirement for managing and addressing identified risks, such as by implementing controls to protect against identified risks.

4.9. UA should fully implement its IT risk assessment process by:

a. Conducting the IT risk assessment in all of its individual units;

b. Compiling and analyzing the results of the IT risk assessment;

c. Using these results to establish a university-wide IT risk profile; and

d. Communicating the results to UA's leadership.

4.10. NAU should continue its efforts to further align its incident response process with IT standards and best practices and ensure its incident response policies and procedures address training for incident response personnel and testing its incident response process, including establishing time frames for training and testing.

4.11. UA should develop and implement policies and procedures for training incident response personnel and for testing its incident response process, including establishing time frames for training and testing.

4.12. UA should develop procedures for assessing whether UA staff are complying with its incident response policies and procedures and take steps to help ensure identified instances of noncompliance are adequately addressed.

ABOR should enhance governance of universities' IT security by expanding oversight activities

The Arizona Board of Regents (ABOR) should enhance its governance of information technology (IT) security at the State's universities—Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA)—by expanding its oversight of IT security using its existing processes. According to governing board guidance published by multiple organizations, including several that provide guidance specifically for higher education governing boards, higher education governing boards play an important role in ensuring universities' IT security risks are adequately identified and addressed and recommend several oversight practices that governing boards can use to increase the effectiveness of their IT security governance. Although ABOR provides some IT security guidance and oversight to the universities, its oversight efforts do not include several of the recommended practices for providing effective IT security governance, and implementing these activities may have helped ABOR and the universities identify and address several of the IT security issues auditors identified. Therefore, ABOR should expand its oversight of the universities' IT security efforts, and because of its limited staff resources, it could use its existing oversight processes for this expanded oversight.

Governing boards play important role in ensuring effective IT security

According to governing board guidance, higher education governing boards play an important role in ensuring universities' IT security risks are adequately addressed, and these organizations recommend various IT security governance oversight activities that governing boards can provide. Specifically, governing guidance published by multiple organizations, including several that provide guidance specifically for higher education governing boards, indicates that these boards should develop an understanding of IT security risks and take steps to help ensure that these risks are adequately addressed.[38] These organizations recommend various oversight practices that governing boards can implement to provide effective IT security governance, including:

- Establishing IT security policies, strategies, and priorities;
- Requiring that organizational IT security investments and improvements be measurable;
- Requiring the organization to monitor and regularly report to the board on IT security program effectiveness and other information, such as any data breaches that have occurred or information demonstrating compliance with key board policies and priorities;
- Requiring annual internal and external audits of the organization's IT security program, including reporting audit results to the board;
- Reviewing the results of the organization's assessment of IT security risks;

[38] Higher Education Information Security Guide. (n.d.) *Information security governance toolkit*. Retrieved from https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Governance; IT Governance Institute. (2006). *Information security governance: Guidance for board of directors and executive management (2nd ed.)* Rolling Meadows, IL; The Association of Governing Boards of Universities and Colleges & United Educators (2014). *A wake-up call: Enterprise risk management at colleges and universities today.* Washington, DC & Bethesda, MD.

- Requiring that organizational IT security risk-management plans and activities are aligned with the organization's overall strategic goals; and
- Obtaining cyber insurance to help pay for the potential costs of data breaches, which may not be covered by existing insurance coverage (see Introduction, pages 3 through 4, for more information on the potential costs of data breaches).

ABOR's IT security governance efforts could be enhanced to include several additional recommended oversight practices that may have helped identify and address IT security issues

ABOR's governance of the universities' IT security efforts has included some of the actions related to IT security recommended for governing boards, but it does not include several of the recommended practices to provide effective IT security governance. Specifically, ABOR has:

- **Established IT security policies and guidelines—**ABOR has developed a policy manual that includes specific guidelines for the universities' IT security efforts. For example, this manual explains that each university president is responsible for assuring that appropriate and auditable information security controls are in place for all university information resources and systems and requires that each university develop, implement, and maintain an information security program.
- **Reviewed and approved the universities' internal audits, including some that have assessed IT security practices—**ABOR's audit committee reviews and approves each university's annual internal audit plans and reports of various operational areas. These audit plans are based on each university's annual risk assessment, which is conducted by internal auditors at each university. In fiscal years 2016 and 2017, the universities' internal audits addressed some IT security topics, such as IT physical security at ASU, IT general controls at NAU, and mobile computing security at UA.
- **Worked with the universities to secure cyber insurance—**ABOR reported working with each university to secure cyber insurance to help pay for the costs associated with a data breach.[39] These insurance policies went into effect in early 2017 and were renewed in April 2018. ASU and UA have insurance policies that provide up to $20 million in coverage, and NAU has a single policy that provides up to $10 million in coverage.[40]
- **Required reporting of security breaches—**ABOR policy requires that if one of the universities determines that a security breach has likely occurred that involves access to and/or the acquisition of personal information, the university should promptly report the incident in writing to both ABOR's chair and president.

However, ABOR's IT security governance efforts have not included several of the recommended oversight practices governing boards can implement to provide effective IT security governance. Implementing these practices may have helped ABOR and the universities identify and address some of the issues identified by auditors as previously discussed in Finding 2 (see pages 11 through 26), Finding 3 (see pages 27 through 35), and Finding 4 (see pages 37 through 45). For example, ABOR:

- **Does not require universities to regularly report certain IT security information—**ABOR does not require the universities to regularly provide it with certain information related to IT security, such as IT security strategic plans, information on IT security program effectiveness, information about security incidents that have occurred that do not constitute security breaches, or information demonstrating compliance with key ABOR IT policies and priorities. Requiring the universities to regularly report this IT security information may have helped ABOR and the universities address several issues previously discussed in this report, such

[39] These insurance policies provide coverage for costs related to data breach response and management, data recovery, cyber-extortion, business interruption, insurance claims, damage claims, and regulatory expenses and fines.

[40] ASU's and UA's policies provide $10 million in coverage and both universities also purchased additional policies providing up to another $10 million in coverage.

as NAU's and UA's lack of IT security strategic plans, lack of monitoring processes for IT security program effectiveness and third-party compliance with contract requirements related to IT security, and the small number of staff dedicated to developing and updating university-wide IT security policies and guidance at UA (see Finding 3, pages 27 through 35).

- **Does not require annual IT security audits—**Although ABOR's audit committee reviews and approves each university's annual internal audit plans and reports, it does not require the universities to conduct annual internal audits or contract for external audits of their IT security practices. Instead, it relies on each university's internal auditors to develop annual audit plans, which ABOR's audit committee reviews and approves. However, EDUCAUSE recommends that university governing board audit committees establish the need for and timing of IT security audits. Requiring regularly scheduled IT security audits may have helped ABOR and the universities identify and address several issues previously discussed in this report, such as deficiencies in existing IT security policies at all three universities and university staff not consistently following university policies (see Finding 2, pages 11 through 26, for more information).

- **Does not review or participate in universities' IT risk assessments—**Although ABOR receives the universities' annual risk assessments, which may include identified IT-related risks, ABOR does not require the universities to submit a dedicated IT security risk assessment. Doing so may have helped ABOR and the universities identify and address issues related to IT risk assessments previously discussed in this report (see Finding 4, pages 40 through 42, for more information).

ABOR should expand its IT security oversight using existing processes

To help ensure the universities develop and implement appropriate IT security programs, ABOR should work with the universities to develop and implement a comprehensive plan for expanding its governance and oversight of the universities' IT security practices. As part of expanding its efforts in this area, ABOR should consider implementing additional oversight practices recommended for governing boards, including:

- Requiring the universities to monitor and regularly report to ABOR on IT security program effectiveness;

- Requiring each university's annual audit plan to include an IT security component, such as audits of specific IT security controls or processes, including reporting audit results to ABOR; and

- Reviewing the results of the universities' IT risk assessments.

According to ABOR, it has limited staff resources for conducting these oversight practices, which has limited the amount of IT security oversight it can provide. Therefore, ABOR could incorporate expanded IT security oversight practices into its existing university oversight processes. For example, ABOR requires ASU, NAU, and UA to annually update ABOR on their business plans, budget, and progress toward meeting strategic goals through their annual Operational and Financial Reviews (OFR). As part of these OFRs, each university submits a written report, which it further supplements with a university presentation during an ABOR meeting. ABOR could incorporate requirements for the universities to report IT security information through these OFRs, including information on IT security program expenses, investments, and effectiveness; any security incidents that have occurred in the previous year; information demonstrating compliance with key ABOR IT security policies and priorities; and results of the universities' IT risk assessments. Additionally, to help ensure that the universities develop IT security strategic plans that are aligned with both ABOR's and the universities' overall strategic goals, ABOR could consider establishing strategic goals for IT security as part of its strategic planning process, which includes working with the universities to establish strategic goals in several areas (see Finding 3, pages 27 through 35, for more information about IT security strategic plans). For example, since 2008, one of ABOR's strategic priorities has been to increase the number of Arizonans with a college degree, and ABOR has worked with the universities to establish several student retention and graduation goals for each university related to this priority.[41]

[41] See Auditor General report 18-102 *Arizona's universities: Student success*.

Finally, ABOR could expand the IT security oversight activities of its audit committee. For example, the audit committee could require the universities to annually conduct internal audits and/or contract for external audits of their IT security programs, report audit results to the audit committee, and/or require the universities to regularly report IT security information to the audit committee, such as results of the universities' IT risk assessments.

Recommendation

5.1. ABOR should work with the universities to develop and implement a comprehensive plan for expanding its governance and oversight of the universities' IT security practices. As part of expanding its efforts in this area, ABOR should consider implementing additional oversight practices recommended for governing boards, including:

a. Requiring the universities to monitor and regularly report to ABOR on IT security program effectiveness;

b. Requiring each university's annual audit plan to include an IT security component, such as audits of specific IT security controls or processes, including reporting audit results to ABOR; and

c. Reviewing the results of the universities' IT risk assessments.

Methodology

Auditors used various methods to study the issues addressed in this report. These methods included reviewing applicable federal and state laws; interviewing staff from the Arizona Board of Regents (ABOR), Arizona State University (ASU), Northern Arizona University (NAU), and the University of Arizona (UA); reviewing the universities' and ABOR's information technology (IT) policies and procedures, information provided by university staff, and information obtained from the universities' and ABOR's websites; and reviewing information on IT breaches and IT definitions.

In addition, auditors used the following specific methods to meet the audit objectives:

- To evaluate the security of the universities' IT systems and data, auditors performed simulated social engineering attacks and analyzed the universities' policies, procedures, and other documents related to information security awareness training and compared them to IT standards and best practices published by the National Institute of Standards and Technology (NIST).[42] In addition, auditors and an independent security consultant retained by the Office of the Auditor General tested university applications and networks using both automated and more detailed security testing techniques. To identify the number and type of the universities' IT systems, auditors interviewed university staff, reviewed documents, and performed technical scanning techniques. Using a risk-based approach, auditors and the security consultant selected various IT systems to test with automated and manual methods. These methods identified potential vulnerabilities in the applications and associated network servers, and auditors and the security consultant selected some IT systems for further detailed testing. This testing allowed auditors to identify the potential risk that these applications might be compromised because of their vulnerabilities. Further, auditors assessed the appropriateness of the universities' various security processes by analyzing their IT security policies and procedures in five areas and comparing them to IT standards and best practices published by NIST and the Open Web Application Security Project.[43] Auditors also reviewed internal control best practices published by the U.S. Government Accountability Office (see Finding 2, page 21, for the citation). Finally, auditors interviewed staff in at least one college, department, or business unit (unit) at each university to help determine the extent the unit(s) followed university-wide policies and procedures.[44] Because of the information's sensitive nature, specific information about the security weaknesses identified and the methods used to identify them has been excluded from this report and shared only with appropriate university officials.

---

[42] Wilson, M., & Hash, J. (2003). *NIST Special Publication 800-50: Building an information technology security awareness and training program*. Gaithersburg, MD: National Institute of Standards and Technology.

[43] National Institute of Standards and Technology (NIST). (2013). *NIST Special Publication 800-53, Revision 4: Security and privacy controls for federal systems and organizations*. Gaithersburg, MD; Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *NIST Special Publication 800-115: Technical guide to information security testing and assessment*. Gaithersburg, MD: National Institute of Standards and Technology; Open Web Application Security Project (OWASP). (2014). *Testing guide, version 4.0*. Bel Air, MD: OWASP Foundation; Open Web Application Security Project (OWASP). (2017a). *OWASP top 10-2017: The ten most critical web application security risks*. Bel Air, MD: OWASP Foundation; Open Web Application Security Project (OWASP). (2017b). *Code review guide 2.0*. Bel Air, MD: OWASP Foundation.

[44] Auditors selected individual units for review at ASU and NAU by first having university officials identify the individual units that operate to some extent independently from their respective central IT offices that are responsible for university-wide development and use of information technology. Next, auditors judgmentally selected 1 of the 18 individual units ASU officials identified and 1 of the 10 individual units that an NAU official identified, based on risk factors such as the number of staff in the unit and the percentage of staff that had not completed the required security awareness training. Because all UA individual units operate relatively independent of UA's central IT office, auditors sampled 6 of its 63 total reported individual units. Specifically, auditors first identified all individual units with 50 or more staff, then identified the remaining individual units where more than two-thirds of unit staff had not completed UA's security awareness training. Then, auditors randomly selected 6 of the remaining individual units.

- To determine if the universities had established appropriate university-wide IT security governance frameworks, auditors analyzed various university documents related to IT security governance, including strategic planning documents, policies, procedures, and other guidance documents, and documents related to the universities' efforts to monitor the effectiveness of and compliance with their IT security policies and procedures, and compared them to IT standards and best practices published by EDUCAUSE, the Higher Education Information Security Council, and NIST (see Finding 3, pages 27 through 35, for specific citations).

- To determine if the universities had established adequate policies and procedures for data classification, IT risk assessment, and incident response, auditors reviewed the universities' policies, procedures, and other documents and compared them to IT standards and best practices published by the International Organization for Standardization and NIST (see Finding 4, pages 37 through 45, for specific citations). Further, auditors reviewed university documentation related to implementing these policies and procedures.

- To evaluate ABOR governance of the universities' IT security practices, auditors interviewed ABOR staff, and reviewed ABOR's policy manual and meeting minutes. Auditors compared ABOR's oversight activities to best practices from the Association of Governing Boards of Universities and Colleges, the Higher Education Information Security Council, and the IT Governance Institute (see Finding 5, page 47, for specific citations).

- Auditors' work on internal controls included reviewing and assessing the universities' and ABOR's policies and procedures and performing the test work described in the previous bullets. Auditors' conclusions on internal controls are reported in Findings 1, 2, 3, 4, and 5 of the report.

Auditors conducted this performance audit of the State's universities in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Auditor General and staff express appreciation to ABOR's chair, members, interim managing director, and staff and ASU's, NAU's, and UA's presidents and staff for their cooperation and assistance throughout the audit.

RESPONSES

2020 N. Central Avenue, Suite 230
Phoenix, Arizona 85004
P 602.229.2500
F 602.229.2555
AZRegents.edu

BOARD OF Regents ARIZONA'S PUBLIC UNIVERSITIES
EDUCATE · DISCOVER · IMPACT

June 18, 2018

Lindsey Perry
Auditor General
2910 N. 44th Street
Phoenix, AZ 85018

Dear Auditor General Perry:

On behalf of the Arizona Board of Regents, I am pleased to respond to the audit report, Arizona's Universities – Information Technology Security. First, let me thank you and your audit team for their utmost professionalism and integrity in reviewing our practices and in developing their findings. They are thoughtful and represent months of collaborative work.

The findings are agreed to and the audit recommendations will be implemented.

The regents will not only work to implement our findings, but will also monitor the implementation of the university specific findings. We are constantly looking for ways to improve and appreciate your help in that endeavor.

Sincerely,

John Arnold
Interim Managing Director

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1 – 1.5: Not applicable to ABOR.

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1 – 2.3: Not applicable to ABOR.

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1 – 3.3: Not applicable to ABOR.

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1 – 4.12: Not applicable to ABOR.

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: ABOR should work with the universities to develop and implement a comprehensive plan for expanding its governance and oversight of the universities' IT security practices. As part of expanding its efforts in this area, ABOR should consider implementing additional oversight practices recommended for governing boards, including:

Recommendation 5.1a: Requiring the universities to monitor and regularly report to ABOR on IT security program effectiveness;

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

Recommendation 5.1b: Requiring each university's annual audit plan to include an IT security component, such as audits of specific IT security controls or processes, including reporting audit results to ABOR; and

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

Recommendation 5.1c: Reviewing the results of the universities' IT risk assessments.

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

ARIZONA STATE UNIVERSITY

June 18, 2018

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

Dear Ms. Perry:

On behalf of Arizona State University (ASU), I am pleased to respond to the performance audit of Information Technology Security at ASU. We are in agreement with all of your findings and our responses to your recommendations are enclosed.

My staff and I wish to thank you and your staff for the professional manner in which this audit was performed. We are constantly looking for ways to improve our program and operations.

Sincerely,

Michael M. Crow
President

Enclosure

cc: Mark Searle, Executive Vice President and University Provost
Morgan R. Olsen, Executive Vice President and CFO

OFFICE OF THE PRESIDENT
FULTON CENTER 410, 300 E. UNIVERSITY DRIVE
PO BOX 877705 TEMPE, AZ 85287-7705
(480) 965-5253 FAX: (480) 965-0865
HTTP://PRESIDENT.ASU.EDU

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1: ASU should develop and implement written policies and procedures that:

Recommendation 1.1a: Specify roles and responsibilities for monitoring employee compliance with security awareness training;

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

Response explanation: ASU added the annual training requirement that was documented in the New Employee Orientation Guidance to our existing Information Security Policy and created a Security Awareness Compliance Procedure that includes roles and responsibilities for monitoring employee compliance with security awareness training. This was completed May 2018.

Recommendation 1.1b: Include a requirement for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so;

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

Response explanation: The security awareness training completion rate included in the report is as of March 2018 and represents an in-process training campaign. Security awareness training is tracked on an annual basis with training required to be complete by June 30, 2018. ASU created a Security Awareness Compliance Procedure that includes a requirement for regularly using the ASU training dashboard to review employees' completion and to report noncompliance to the Accountable Administrator. This was completed May 2018.

Recommendation 1.1c: Specify requirements for following up with employees who have not completed the required training; and

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

Response explanation: ASU created a Security Awareness Compliance Procedure that includes a requirement for following up with employees who have not completed the required training. This was completed May 2018.

Recommendation 1.1d: Identify potential consequences to employees for not completing required security awareness training within specified time frames, such as warnings and revoked access.

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

Response explanation: Potential consequences are included under the Violations and Enforcement section of the Information Security Policy. This was completed April 2018.

Recommendation 1.2 – 1.5: Not applicable to ASU.

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1: ASU should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

Recommendation 2.1a: Developing and implementing additional written policies and procedures for its vulnerability management process that include requirements and/or guidance for:

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;
- Sharing scan results across the university to help eliminate similar vulnerabilities in other IT systems;
- Conducting penetration testing at specified frequencies based on risk;
- Using its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and
- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

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

Response explanation: ASU has a long-standing commitment to vulnerability remediation training, including a bi-weekly training session for vulnerability management, and will incorporate sharing remediation techniques for common vulnerabilities into this training agenda. ASU will update its existing Web Application Vulnerability Standard to address penetration testing. Additionally, ASU is creating a separate Network Vulnerability Standard that will include the network recommendations suggested by audit

to improve the regular scanning process of ASU's network. The expected completion date is July 2018.

Recommendation 2.1b: Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

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

Response explanation: ASU has a Server Security Standard and detailed endpoint security guidelines in place today and will supplement this documentation with additional detailed configuration best practices for network-attached devices. This documentation is scheduled to be reviewed and updated annually. ASU continues to investigate endpoint management tools to reduce further vulnerabilities stemming from inappropriate configurations. The expected completion date for new documentation is July 2018.

Recommendation 2.1c: Developing and implementing additional patch management policies and procedures to include guidance on how its staff should identify system flaws requiring patches and requirements for reporting those flaws to appropriate individuals for remediation.

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

Response explanation: ASU has a Patch Management Standard in place today. We will incorporate additional guidance in utilizing patching documentation available for reference in identifying known issues as part of the vulnerability management best practices. The expected completion date for new documentation is July 2018.

Recommendation 2.1d: Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Using secure coding standards when developing web applications;
- Requiring web application developers to be trained on developing secure software;
- Reviewing web application source code before web applications are released; and
- Performing security testing before web applications are released.

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: ASU currently requires these activities for all web applications with a criticality rating of High and Medium and recommends this activity for the Low criticality ratings. ASU will formalize its existing ad hoc training program in place today and implement a program to provide annual training for developers who administer web applications with a criticality rating of High or Medium. The expected availability for the new training is January 2019.

Recommendation 2.1e: Developing and implementing policies and procedures for protecting system logs from unauthorized access, modification, and deletion.

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

Response explanation: ASU has a System Audit Standard that currently requires logging to use a tamper-resistant mechanism. ASU will strengthen the language to clarify log management where separation of duties is a factor. In addition, ASU continues to recommend centralized logging via our enterprise logging solution that is currently available. The expected completion date for the revised standard is July 2018.

Recommendation 2.1f: Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

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

Response explanation: This spring ASU implemented a process to provide executive dashboard review with all Accountable Administrators. We have updated our risk assessment standard to document this new process. We also will continue to require expanded centralized logs for critical systems which allows visibility and stronger centralized oversight.

Recommendation 2.2 – 2.3: Not applicable to ASU.

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1 – 3.2: Not applicable to ASU.

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1: ASU should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified.

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: ASU's current Secure Development Standard requires a centralized inventory for High and Medium Criticality-rated systems. ASU will continue to centrally maintain this ASU-wide inventory and additionally recommend that departments and units include Low criticality systems. The inventory will include the required data elements – data classification, data owner and data description. During the ASU-wide annual review of High and Medium criticality systems, next scheduled January 2019, ASU will reinforce that departments must maintain their inventory. The revised standard is expected to be released by July 2018.

Recommendation 4.2: ASU should:

Recommendation 4.2a: Establish time frames and guidance for regularly reviewing and updating data inventories; and

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: See Recommendation 4.1 response.

Recommendation 4.2b: Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

ASU Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: See Recommendation 4.1 response.

Recommendation 4.3 – 4.12: Not applicable to ASU.

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: Not applicable to ASU.

NORTHERN ARIZONA UNIVERSITY | Office of the President

nau.edu/president
presidentsofficesupport@nau.edu

928-523-3232 office
928-523-1848 fax
P.O. Box 4092
Flagstaff, AZ 86011

June 18, 2018

Lindsey Perry
Auditor General
Office of the Auditor General
2910 N. 44th Street, Suite 410
Phoenix, AZ 85018

RE: Response to Auditor General's Report on Arizona's public universities' information technology security

Dear Ms. Perry:

This letter provides Northern Arizona University's response to the Audit Report on the universities' information technology security.

Information security resources impact nearly every aspect of the NAU mission, vision, and values and as such, protection of those resources is important to NAU. This audit reaffirms the work NAU has already accomplished to develop and implement strong IT security policies, procedures, and practices. This audit also identifies opportunities where we can apply the same practices more specifically to other information security goal and objective areas. We appreciate this Office of the Auditor General feedback as we strive to further enhance our efforts to improve our information security posture, ensure our students' success, and help advance Arizona's educational attainment levels.

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1: Not applicable to NAU.

Recommendation 1.2: NAU should finish developing and implement its draft security awareness training policies and procedures, including adding requirements for regularly using an automated tracking system for analyzing all employees' security awareness training

completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its draft security awareness training policies and procedures.

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

Response explanation: NAU has completed the development and implementation of its security awareness training policy and procedures. This includes the requirements for tracking and reporting on completion, reporting (via email) noncompliance, and establishing time frames for compliance. This was completed in June 2018.

Recommendation 1.3: NAU should specify a time frame for new employees to complete initial security awareness training within its policies and procedures.

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

Response explanation: NAU specifies a time frame for new employees to complete initial security awareness training within its policy and procedures. The policy states new employees shall complete the training within sixty (60) days. This was completed in June 2018.

Recommendation 1.4 – 1.5: Not applicable to NAU.

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1: Not applicable to NAU.

Recommendation 2.2: NAU should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

Recommendation 2.2a: Finishing development of and implementing its draft policies and procedures establishing a vulnerability scanning process.

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

Response explanation: NAU will complete the development and implementation of its policies and procedures establishing a vulnerability scanning process.

Recommendation 2.2b: Developing and implementing additional written university-wide policies and procedures for penetration testing that include:

- Requirements for conducting penetration testing at specified frequencies based on risk.
- Guidance for its risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be considered for

conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and

- Guidance for helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all higher-risk web applications.

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

Response explanation: NAU will develop and implement written university-wide policies and procedures for penetration testing that includes industry best practices.

Recommendation 2.2c: Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

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

Response explanation: NAU will develop and implement revised configuration management policies and procedures that include IT standards and best practices.

Recommendation 2.2d: Revising its configuration management policies and procedures to indicate that they apply to all NAU IT systems.

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

Response explanation: NAU will revise configuration management policies and procedures to indicate that they apply to all NAU IT systems.

Recommendation 2.2e: Finishing development of and implementing its draft patch management policies and procedures.

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

Response explanation: NAU will complete the development and implementation of patch management policies and procedures.

Recommendation 2.2f: Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Gathering web application security requirements when developing web applications;

- Using secure coding standards when developing web applications;
- Requiring web application developers to be trained on developing secure software;
- Conducting threat modeling during web application development or security testing before releasing web applications to the live environment;
- Reviewing web application source code for web applications it develops internally before these web applications are released; and
- Performing security testing before web applications are released.

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

Response explanation: NAU will develop and implement additional web application development policies and procedures that include IT standards and best practices.

Recommendation 2.2g: Developing and implementing written log monitoring policies and procedures that:

- Describe the critical IT systems and functions within each IT system that should be logged;
- Specify how frequently each log should be monitored;
- Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
- Require analysis of security-related information generated by log monitoring across the university to determine any patterns that might indicate a potential attack;
- Outline standard response actions for specific types of detected events, including informing designated personnel of security risks to the university and to individual IT systems; and
- Include requirements for securely protecting the logs, including protecting them from unauthorized access, modification, and deletion, and time frames for how long to retain the logs before deleting them.

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

Response explanation: NAU will continue to develop and implement written log monitoring policies, standards, and procedures that align with industry best practices.

Recommendation 2.2h: Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including the development of corrective action plans, provision of training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

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

Response explanation: NAU will continue to develop and implement university-wide

policies and procedures for reporting, evaluating, and correcting instances of noncompliance with IT security policies and procedures.

Recommendation 2.3: Not applicable to NAU.

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1: NAU should:

Recommendation 3.1a: Finish developing and implement its draft IT security strategic plan including developing a mission, goals, and objectives aligned with NAU's overall strategic mission, and performance measures to assess progress toward achieving those objectives.

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

Response explanation: NAU will complete the development and implementation of the IT security strategic plan.

Recommendation 3.1b: Finish developing and implement its draft information security policy and draft information security program, including outlining how its policies and IT security controls should be communicated to those responsible for implementing them.

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

Response explanation: NAU will complete the development and implementation of the information security policy and information security program.

Recommendation 3.1c: Develop and implement policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

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

Response explanation: NAU will develop and implement policies and procedures for monitoring the effectiveness of the IT security practices and use monitoring results to help inform security policy and procedure revisions.

Recommendation 3.1d: Develop and implement policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security.

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

Response explanation: NAU will develop and implement policies and procedures to monitor and assess third parties' adherence to contractual agreement requirements as

related to IT security.

Recommendation 3.2: Not applicable to NAU.

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1 – 4.2: Not applicable to NAU.

Recommendation 4.3: NAU should revise its data classification policies and procedures to include a requirement to periodically review its classification of data to ensure the data is appropriately classified and to update its data inventory, as necessary.

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

Response explanation: NAU will revise the data classification policies and protocols to include a requirement to periodically review the classification of data.

Recommendation 4.4: NAU should develop a plan for implementing its data classification policies and procedures, including:

Recommendation 4.4a: Establishing a deadline by which all individual units must complete the data classification process and develop data inventories; and

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

Response explanation: NAU will establish a deadline by which all units must complete the data classification process.

Recommendation 4.4b: Following up with individual units to ensure they have completed the process.

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

Response explanation: NAU will follow up with units to ensure completion of the data classification process.

Recommendation 4.5 – 4.6: Not applicable to NAU.

Recommendation 4.7: NAU should develop and implement university-wide IT risk assessment policies and procedures for conducting IT risk assessments, compiling and evaluating the results, using the results to manage and address identified risks, such as by implementing controls to protect against identified risks, and reporting the results to NAU's leadership. Additionally, the policies and procedures should assign roles and responsibilities for conducting and completing these various requirements and procedures.

NAU Response: The finding of the Auditor General is agreed to and the audit

recommendation will be implemented.

Response explanation: NAU will develop and implement university-wide IT risk assessment policies and procedures for conducting IT risk assessments in alignment with best practices.

Recommendation 4.8 – 4.9: Not applicable to NAU.

Recommendation 4.10: NAU should continue its efforts to further align its incident response process with IT standards and best practices and ensure its incident response policies and procedures address training for incident response personnel and testing its incident response process, including establishing time frames for training and testing.

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

Response explanation: NAU will continue to further align the incident response process with IT standards and best practices.

Recommendation 4.11 – 4.12: Not applicable to NAU.

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: Not applicable to NAU.

NAU Response: This response will be provided by ABOR.

Sincerely,

Rita Hartung Cheng
President

THE UNIVERSITY OF ARIZONA
Executive Office of the President

1200 E. University Blvd. Rm. 200
P.O. Box 210021
Tucson, AZ 85721-0021

Off: 520-621-5511
Fax: 520-621-9323

president.arizona.edu

June 18, 2018

Lindsey Perry, Auditor General
State of Arizona - Office of the Auditor General
2910 N 44th Street- Suite #410
Phoenix, AZ 86018

Dear Ms. Perry,

I have reviewed the preliminary report of the ***Arizona's Universities - Information Technology Security*** performance audit. Thanks to you and your team for the work that has been put into the audit and for engaging us in a dialogue about how we can better secure our network, systems, and data. The report clearly values the work we have done at the University of Arizona by showing that UA has:

- Acted quickly to make information security improvements by appointing a CIO.
- A culture of security awareness as evidenced by the predominantly positive results of the audit social engineering tests.
- The ability to further improve our security posture by employing automated security tools, network segmentation, a risk assessment process, and other effective tools and processes.

The report highlights a number of areas where the University of Arizona can improve and expand its efforts. We agree with the findings overall, agree to the recommendations and moving forward with the work.

There are several campus leaders that worked hard throughout this process to make this report possible. They spent hours collecting and sharing key data and ensured that the University of Arizona responded to requests from your office in a timely manner. I would be remiss if I did not recognize that hard work, including the efforts of:

- Dr. Allison Vaillancourt, Vice President for Business Affairs and Human Resources, and Audit Coordinator
- Dr. Jeff Goldberg, Acting Provost
- Gregg Goldman, Senior Vice President, Business Affairs and CFO
- Karen Williams, Vice President for Information Strategy and University Libraries
- Barry Brummund, Chief Information Officer
- Lanita Collette, Chief Information Security Officer

This group will provide leadership as we move forward to address the recommendations outlined in the report.

Thank you once again for the thorough review of our information security efforts.

Sincerely,

Robert C. Robbins, MD
President

Finding 1: Relatively few university employees susceptible to simulated social engineering attacks, but universities should improve security awareness training

Recommendation 1.1 – 1.3: Not applicable to UA.

Recommendation 1.4: UA should implement its security awareness training policy and develop and implement additional policies or procedures for regularly using an automated tracking system for analyzing all employees' security awareness training completion and reporting noncompliance to those responsible for enforcing compliance, including establishing time frames for doing so; and following up with employees who have not completed the required security awareness training and taking corrective action, such as enforcing the consequences identified in its security awareness training policy.

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

Recommendation 1.5: UA should revise its security awareness training policies and procedures to require existing employees to complete security awareness training annually, define the roles and responsibilities of staff who will develop and implement security awareness training materials, and include requirements for periodically evaluating and updating security awareness training materials.

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

Finding 2: Universities should enhance IT security controls to further protect IT systems and data

Recommendation 2.1 – 2.2: Not applicable to UA.

Recommendation 2.3: UA should enhance its existing IT security policies and procedures to fully align them with IT standards and best practices, including considering the use of risk-based approaches, where appropriate, by:

Recommendation 2.3a: Developing and implementing revised policies and procedures for its vulnerability management process that include requirements and/or guidance for:

- Regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors such as the amount and nature of sensitive data contained in certain IT systems and web applications, and the extent that scanning is used to assess whether individual units are identifying and addressing vulnerabilities, such as configuration and patch-related vulnerabilities;
- Analyzing scan results, including specifying time frames for conducting the reviews, and sharing these results across the university to help eliminate similar vulnerabilities in other IT systems;
- Conducting penetration testing at specified frequencies based on risk;
- Using a risk-based approach for conducting penetration testing for the IT systems on its network and its web applications, including specifying risk factors that should be

considered for conducting this testing, the frequency at which risks will be assessed, and procedures for conducting penetration testing based on identified risks; and

- Helping to ensure all higher-risk web applications are tested within a specified time frame, such as determining whether to allocate additional resources for penetration testing or reducing the scope or frequency of penetration tests for some or all high-risk web applications.

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

Recommendation 2.3b: Developing and implementing revised configuration management policies and procedures that include the following IT standards and best practices:

- Detailed guidance for how to configure IT systems so that these IT systems only provide essential capabilities and prohibit or restrict the use of certain functions, or requirements for developing baseline configurations, which provide a standard set of specifications for configuring all IT systems;
- Defining the frequency of reviews and updates to IT system configurations; and
- Using unique settings for configuring IT resources to limit broad access across IT systems.

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

Recommendation 2.3c: Developing and implementing additional patch management policies and procedures that include the following:

- Identifying needed patches, reporting those patches to appropriate individuals responsible for remediation, and applying patches;
- Testing patches for effectiveness and potential side effects before installation; and
- Installing patches within required time frames.

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

Recommendation 2.3d: Developing and implementing additional web application development policies and procedures that include the following IT standards and best practices:

- Requiring web application developers to be trained on developing secure software;
- Reviewing web application source code before web applications are released; and
- Performing security testing before web applications are released.

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

Recommendation 2.3e: Developing and implementing additional log monitoring policies and procedures that include the following requirements and guidance:

- Specifying how frequently each log should be monitored;

- Identifying who is responsible for ensuring log events are captured and reviewing log events on a regular basis;
- Analyzing security-related information generated by log monitoring across the university to determine any patterns that might indicate potential attack; and
- Including requirements for securely protecting the logs and time frames for how long to retain the logs before deleting them.

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

Recommendation 2.3f: Developing and implementing university-wide policies and procedures for:

- Reporting identified noncompliance with IT security policies and procedures to individuals responsible for implementation and oversight of IT security policies and procedures;
- Evaluating instances of noncompliance to determine if and how to address them and documenting why any noncompliance will not be addressed; and
- Correcting issues in a timely manner, including developing corrective action plans, providing training, and other steps to address the identified issues, as appropriate, and documenting the corrective actions.

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

Recommendation 2.3g: Developing and implementing university-wide procedures aligned with best practices that all individual units must follow when developing policies and procedures to address the recommendations in this finding; or include sufficient guidance in its university-wide policies to help ensure its individual units develop procedures for implementing UA's policies that fully align with IT standards and best practices.

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

Finding 3: ASU has established an appropriate IT security governance framework, and NAU and UA should continue to improve and develop IT security governance

Recommendation 3.1: Not applicable to UA.

Recommendation 3.2: UA should develop and implement:

Recommendation 3.2a: An IT security strategic plan that contains a mission, goals, and objectives aligned with UA's overall strategic mission and includes performance measures to assess progress toward achieving those objectives.

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

Recommendation 3.2b: IT security policies and guidance documents that explain how UA will guide the management and protection of its IT systems and the data contained in them,

such as developing an information security program that outlines its overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls and explains how it will communicate UA's policies and IT security controls to those responsible for implementing them.

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

Recommendation 3.2c: Policies and procedures for monitoring the effectiveness of its IT security practices, identifying areas of policy noncompliance, and using monitoring results to inform revisions to its IT security policies and procedures.

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

Recommendation 3.2d: Policies and procedures to monitor and assess third parties to ensure that they are adhering to contractual or agreement requirements related to IT security.

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

Finding 4: Universities should improve processes in three key information security program areas

Recommendation 4.1 – 4.4: Not applicable to UA.

Recommendation 4.5: UA should revise its data classification policies and procedures to require each individual unit to develop a data inventory for its IT systems as part of its data classification process, periodically review its classification of data to ensure the data is appropriately classified, and update its data inventory as necessary. The data inventory should include the data's classification level, identity of the data owner, and a brief description of the data classified.

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

Recommendation 4.6: UA should:

Recommendation 4.6a: Establish time frames and guidance for regularly reviewing and updating data inventories; and

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

Recommendation 4.6b: Develop and implement a plan for ensuring its individual units complete data inventories, including establishing a deadline by which all individual units must complete a data inventory and follow-up procedures to ensure all individual units have done so.

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

Recommendation 4.7: Not applicable to UA.

Recommendation 4.8: UA should revise its IT risk assessment policies and procedures to include a requirement for managing and addressing identified risks, such as by implementing controls to protect against identified risks.

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

Recommendation 4.9: UA should fully implement its IT risk assessment process by:

Recommendation 4.9a: Conducting the IT risk assessment in all of its individual units;

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

Recommendation 4.9b: Compiling and analyzing the results of the IT risk assessment;

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

Recommendation 4.9c: Using these results to establish a university-wide IT risk profile; and

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

Recommendation 4.9d: Communicating the results to UA's leadership.

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

Recommendation 4.10: Not applicable to UA.

Recommendation 4.11: UA should develop and implement policies and procedures for training incident response personnel and for testing its incident response process, including establishing time frames for training and testing.

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

Recommendation 4.12: UA should develop procedures for assessing whether UA staff are complying with its incident response policies and procedures and take steps to help ensure identified instances of noncompliance are adequately addressed.

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

Finding 5: ABOR should enhance governance of universities' IT security by expanding oversight activities

Recommendation 5.1: Not applicable to UA.


ARIZONA
Auditor General
Making a Positive Difference