ARIZONA Auditor General
Making a Positive Difference

Arizona's Universities Information Technology Security
66-Month Follow-Up Report

The June 2018 Arizona's Universities—Information Technology Security performance audit found that the Universities have implemented several information technology (IT) security practices and can further improve IT security, policies, procedures, and practices. We made 3 recommendations to the Arizona Board of Regents (ABOR), 13 recommendations to Arizona State university (ASU), 19 recommendations to Northern Arizona university (NAU), and 23 recommendations to the University of Arizona (UA), and their status in implementing the recommendations is as follows:

Status of ABOR's recommendations

Implemented	3

Status of ASU's recommendations

Implemented	9
Partially implemented	4

Status of NAU's recommendations

Implemented	17
Partially implemented	2

Status of UA's recommendations

Implemented	5
Partially implemented	12
Not implemented	6

As indicated above, ASU, NAU, and ABOR have implemented or partially implemented all the recommendations directed to them. However, as we previously reported in our 48-month followup, although UA had implemented or partially implemented 17 of the recommendations directed to it, it had not implemented 6 recommendations and had not made further progress toward implementing these recommendations since the 24-month followup. Because UA did not outline a plan or estimated time frame for implementing these 6 recommendations, we have not continued to follow up with UA since the 48-month followup. Therefore, unless otherwise directed by the Joint Legislative Audit Committee, this report concludes our follow-up work on the Universities' efforts to implement the recommendations from the June 2018 report.

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

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;

Implemented at 6 months

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;

Implemented at 6 months

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

Implemented at 6 months

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

Implemented at 6 months

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.

Implemented at 24 months

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

Implemented at 6 months

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.

Not implemented—As reported in our 48-month followup, UA had not made further progress toward implementing this recommendation since the 24-month followup. Specifically, UA developed a security awareness training policy that requires all users with access to university information resources to complete security awareness training within the first 30 days from date of hire. Additionally, the policy requires all users to complete an annual refresher training. UA reported in the 24-month followup that it had developed draft procedures for assessing compliance with the annual security awareness refresher training requirement, which included a timeline for generating reports to review compliance and a time frame for restricting user access to the university's network if training has not been completed. UA reported that, as of the beginning of fiscal year 2022, 91 percent of full-time employees, 71 percent of part-time employees, and 30 percent of contractors with access to university information resources had completed security awareness training during the previous year, as required by the policy. We also identified several employees and contractors who did not take the required security awareness training whose job titles indicated they may have access to sensitive data, including a systems administrator, a network engineer, and senior staff in human resources and student services. As of July 2022, UA had not implemented policies, procedures, or other processes for 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. Instead, according to UA, each individual unit is responsible for monitoring its own security awareness training completion rates. Additionally, UA reviews its training completion rates for individual units annually and contacts individual units to inform them if they have low completion rates.

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.

Partially implemented at 24 months—UA's security awareness training policy includes requirements for new users with access to university information resources to complete security awareness training and a requirement for all users to complete refresher training annually. The policy further assigns responsibility for implementing a security awareness training program to the Information Security Office (ISO); however, the policy does not define roles and responsibilities for periodically evaluating and updating security awareness training materials. UA explained that the chief information security officer is ultimately responsible for the information security awareness training program and that not defining roles and responsibilities in policy allows for flexibility to assign tasks on an as-needed basis to ensure appropriate use of personnel for performing duties associated with providing the training.

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

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.

Partially implemented at 24 months—ASU has developed and implemented additional policies and procedures for its vulnerability management process that include requirements and/or guidance for regularly scanning all IT systems on its network and web applications, sharing scan results across the university to help eliminate similar vulnerabilities in other IT systems, and using a risk-based approach for conducting penetration testing for IT systems on its network and web applications, including specifying risk factors that should be considered for conducting this testing. ASU also revised its policies and procedures to indicate it will use a risk-based approach for conducting penetration testing for IT systems on its network and web applications when deemed necessary, including specifying risk factors that would indicate the potential need for conducting penetration testing. However, ASU reported it does not plan to define a specified frequency for conducting penetration testing to ensure all higher-risk web applications are tested within a specified time frame.

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.

Implemented at 24 months

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.

Implemented at 24 months

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.

Implemented at 24 months

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

Implemented at 24 months

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.

Implemented at 24 months

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.

Implemented at 6 months

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.

Partially implemented at 24 months—NAU has implemented a risk-based approach for performing penetration testing of its network IT systems and higher-risk web applications. Although it has established policies that require its higher-risk web applications to be tested at specified frequencies, these policies do not require its network IT systems to be tested at specified frequencies. Rather, network IT systems are tested as needed or upon request. Further, its penetration testing policies and procedures are more closely aligned with a vulnerability management process rather than penetration testing because, although they involve reviewing vulnerability scans to determine if further analysis and validation of the vulnerabilities identified in the scans is necessary, they do not involve exploiting the vulnerabilities, which is a key element of penetration testing.

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.

Partially implemented at 24 months—NAU's Information Technology Services (ITS) department, which is responsible for implementing IT security for most of NAU's individual units, has developed and implemented configuration management policies and procedures that require developing baseline configurations, define the frequency of reviews and updates to the baseline configurations, and require the use of unique settings when configuring IT resources. However, NAU's configuration management policies allow NAU's 5 decentralized units to develop their own configuration settings and/or use pre-built configuration templates provided by third parties. Additionally, the ITS department does not monitor decentralized units to ensure that their configuration settings are consistent with the baseline configurations established in its configuration management policies and procedures. NAU reported that it has accepted the risk of allowing decentralized units to develop their own configuration settings and/or use prebuilt configuration templates and has implemented compensating controls to mitigate the risk of using these templates.

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

Implemented at 24 months

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

Implemented at 6 months

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.

Implemented at 24 months

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.

Implemented at 24 months

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.

Implemented at 6 months

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.

Not implemented—As reported in our 48-month followup, UA had not made progress toward implementing this recommendation since the 24-month followup. Specifically, as reported in the 24-month followup, UA:

- Had developed a Vulnerability Management Standard that required regularly scanning the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors; and analyzing scan results and specifying the time frames for reviewing and sharing the results across the university to help eliminate similar vulnerabilities in other IT systems. However, the standard did not ensure that all IT systems on its network and its web applications were scanned and did not specify the extent that scanning was used to assess whether individual units were identifying and addressing vulnerabilities.
- Had developed a procedure that required 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. However, the procedure did not specify the penetration-testing frequency based on risk and the frequency with which risk would be assessed, outline steps for conducting penetration testing based on identified risk, or include guidance for helping ensure all high-risk web applications are tested within a specified time frame.

As of April 2022, UA had not revised its standards, policies, and/or procedures to address these deficiencies.

In addition, although UA developed a vulnerability management program to provide individual units with optional vulnerability scanning and penetration testing tools and services, many of UA's individual units are responsible for conducting scanning and penetration testing and remediating identified vulnerabilities. UA has also not developed university-wide policies and procedures for identifying and correcting noncompliance with its IT security policies and procedures (see explanation for recommendation 2.3f), including those related to vulnerability management. As a result, individual units have not consistently implemented its vulnerability management standard and penetration testing procedure. For example, we reviewed the implementation of the vulnerability management standard and penetration-testing procedure for a judgmental sample of 3 of UA's 64 individual units and found that 2 units had not fully implemented UA's Vulnerability Management Standard and none had conducted penetration testing.

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.

Not implemented—As reported in our 48-month followup, UA had not made progress toward implementing this recommendation since the 24-month followup. Specifically, as reported in the 24-month followup, UA developed a configuration management policy and procedures requiring all network devices that store, process, or transmit university information of any classification to be securely configured, as well as written procedures for configuring Windows systems, Linux systems, and web applications. The policy and procedures also required the use of unique settings for configuring IT resources to limit broad access across IT systems. However, the policy and procedures lacked sufficiently detailed guidance for configuring IT systems and did not define the frequency of reviews and updates to IT system configurations. As of April 2022, UA had not addressed these deficiencies in its policy and procedures.

Additionally, UA developed a vulnerability management program to provide individual units with services that could identify configuration-related vulnerabilities. However, individual units are responsible for

correcting any identified configuration-related vulnerabilities, and UA has not developed university-wide policies and procedures for identifying and correcting noncompliance with its IT security policies and procedures (see explanation for recommendation 2.3f), including those related to configuration management.

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.

Partially implemented at 48 months—UA has developed a patch management policy and standard, and patch installation and testing guidelines, that require needed patches to be identified and applied, tested before installation, and installed within required time frames. Additionally, UA developed a vulnerability management program to provide individual units with services that could identify patch-related vulnerabilities. However, individual units are responsible for correcting any identified patch-related vulnerabilities, and as previously discussed, UA has not developed university-wide policies and procedures for identifying and correcting noncompliance with its IT security policies and procedures (see explanation for recommendation 2.3f), including those related to patch management.

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.

Partially implemented at 48 months—UA developed web application development policies that require all web application developers to be trained on developing secure software. The policies also require web application developers to review web application source code for all new or significantly modified web applications identified as critical before they are released and perform security testing on all web applications before they are released. UA has also developed a web application development training and, in fiscal year 2021, more than 80 percent of UA's web application developers completed the training. However, UA reported it does not plan to ensure that all web application developers complete the training. Additionally, UA reported that it does not plan to develop a process for assessing business units' compliance with the policy requirements to review web application source code and perform security testing on web applications before they 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.

Not implemented—As reported in our 48-month followup, UA had not made progress toward implementing this recommendation since the 24-month followup. Specifically, as reported in the 24-month followup, UA planned to implement log monitoring policies, standards, and procedures that included the recommended elements by December 2021. However, in April 2022, UA reported that it changed its approach related to logging and monitoring and is planning to move its individual units' servers to a

cloud-based environment that would allow UA's central IT to provide logging and monitoring services for all individual units. UA estimated that it will have all individual units' servers transferred to a cloud-based environment by 2025. In addition, UA was unable to provide documentation showing that it analyzes security-related information generated by log monitoring across the university.

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.

Not implemented—As reported in our 48-month followup, UA had not made further progress toward implementing this recommendation since the 24-month followup. Specifically, as reported in the 24-month followup, UA included a policy-compliance section in each information security policy that outlines responsibility for tracking noncompliance and consequences for some instances of noncompliance, but these policy-compliance sections do not indicate how or to whom instances of noncompliance should be reported or provide details regarding how instances of noncompliance should be evaluated, how unaddressed noncompliance should be documented, or time frames and other steps for addressing noncompliance, such as corrective action plans. As of July 2022, UA reported it does not plan to further revise its university-wide policies and procedures to implement this recommendation because it expects individual unit officials to track and enforce compliance with its IT security policies within their individual units. However, its individual units have not consistently implemented its vulnerability management standard and penetration testing procedure, as required by UA's IT security policies (see explanation for Recommendation 2.3a).

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.

Not implemented—As reported in our 48-month followup, UA had not made further progress toward implementing this recommendation since the 24-month followup. Specifically, as reported in the 24-month followup, UA included a statement in each of its IT security policies indicating that the policy applies university-wide, and it has included similar wording in its IT security program policy; however, implementation of this recommendation was dependent on the implementation of all Finding 2 recommendations. As of April 2022, none of UA's Finding 2 recommendations have been fully implemented (see explanations for Recommendations 2.3a through 2.3f).

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

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.

Implemented at 6 months

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.

Implemented at 6 months

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.

Implemented at 24 months

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.

Implemented at 24 months

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.

Partially Implemented at 48 months—UA has developed an information security strategic plan that contains a mission, goals, objectives, and performance measures to assess progress toward achieving its objectives. UA's information security strategic plan requires each individual unit to develop a security plan for meeting UA's strategic plan objectives. However, in fiscal year 2021, some of UA's individual units did not develop a security plan as required. UA reported that although it has a goal for all its individual units to develop a security plan, it did not have an estimated date for achieving this goal.

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.

Implemented at 24 months

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.

Implemented at 24 months

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.

Implemented at 48 months

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

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 re-view 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.

Partially implemented at 6 months—ASU has developed and implemented policies and procedures requiring its individual units to develop and annually review data inventories that include the data's classification level, identity of the data owner, and a brief description of the data classified for all IT systems classified as high- and medium-criticality. However, as indicated in its response to the performance audit report, ASU has recommended, rather than required, that individual units include IT systems classified as low-criticality in their data inventories, which it reported is consistent with its risk-based approach for IT security. As a result, ASU cannot ensure that it has a full inventory of data residing on its low criticality IT systems, which may prevent it from fully implementing its vulnerability management and web application development policies and procedures. Specifically, ASU's vulnerability management and web application development policies and procedures require ASU staff to periodically and randomly select web applications classified as low-criticality for scanning and security testing. A complete inventory of web applications classified as low-criticality would be necessary for ASU to fully implement its vulnerability management policies and procedures.

4.2 ASU should:

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

Partially implemented at 6 months—ASU has developed and implemented policies and procedures requiring its individual units to annually review and update data inventories for IT systems classified as high- and medium-criticality. However, as indicated in its response to the performance audit report, ASU has recommended, rather than required, that individual units include IT systems classified as low-criticality in their data inventories, which it reported is consistent with its risk-based approach for IT security.

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.

Partially implemented at 6 months—See explanations for Recommendations 4.1 and 4.2a.

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.

Implemented at 6 months

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

Implemented at 24 months

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

Implemented at 24 months

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.

Partially implemented at 24 months—UA requires individual units to complete a risk management process annually, which includes the unit identifying whether it has a complete data inventory. For IT systems that are included in UA's risk management process, individual units should include the data's classification level, identify the data owner, and briefly describe the data. If the individual unit indicates it does not have a complete

data inventory, this is classified as a vulnerability, and UA's risk management process recommends but does not require the individual unit to develop a complete data inventory. However, UA's risk management process indicates that the individual unit may choose to accept the risk of not developing a complete data inventory.

4.6 UA should:

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

Implemented at 24 months

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.

Partially implemented at 48 months—As discussed in the explanation for Recommendation 4.8, UA has implemented a risk management web application for its units to use when completing annually required IT risk assessments. The web application requires individual units to confirm if they have a complete data inventory and, if not, recommends the unit develop a complete data inventory. However, in fiscal year 2021, some of UA's individual units did not complete IT risk assessments using the risk management web application. UA reported that, although it has a goal for all its individual units to complete IT risks assessments using the risk management web application, which could facilitate individual units' development of complete data inventories, it did not have an estimated date for achieving this goal.

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.

Implemented at 24 months

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.

Partially implemented at 48 months—UA has developed IT risk management policies and procedures that require all individual units to complete individual IT risk assessments and develop security plans for implementing controls that address identified risks. However, in fiscal year 2021, some of UA's individual units did not complete individual IT risk assessments or develop security plans, as required. UA reported that, although it has a goal for all its individual units to complete risks assessments and develop security plans, it did not have an estimated date for achieving this goal.

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

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

Partially implemented at 48 months—The 24-month followup reported that UA had implemented this recommendation. However, as discussed in the explanation for recommendation 4.8, in fiscal year 2021, some of UA's individual units did not complete individual IT risk assessments. UA reported that, although it has a goal for all its individual units to complete risks assessments, it did not have an estimated date for achieving this goal.

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

Partially implemented at 48 months—In fiscal year 2021, UA compiled and analyzed the results of its individual units' IT risk assessments. However, as discussed in the explanation for recommendation 4.8, in fiscal year 2021, some of UA's individual units did not complete individual IT risk assessments. UA reported that, although it has a goal for all its individual units to complete risks assessments, it did not have an estimated date for achieving this goal.

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

Partially implemented at 48 months—In fiscal year 2021, UA used the results of its individual units' IT risk assessments to develop a university-wide IT risk profile. However, as discussed in the explanation for recommendation 4.8, in fiscal year 2021, some of UA's individual units did not complete individual IT risk assessments. UA reported that, although it has a goal for all of its individual units to complete risks assessments, it did not have an estimated date for achieving this goal.

d. Communicating the results to UA's leadership.

Implemented at 48 months

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.

Implemented at 24 months

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.

Partially Implemented at 48 months—As reported in the 24-month followup, UA has implemented an incident response policy and plan, but the policy and plan do not address specific training requirements or testing. Instead, UA reported that ongoing incident response training/testing will occur through tabletop exercises twice per year, and UA held 2 tabletop exercises in calendar year 2021. However, UA does not require incident response staff from all its individual units to participate in the tabletop exercises, and it has not developed policies and procedures outlining how it will conduct these exercises. Additionally, although UA has developed incident response training that its IT personnel are required to take, the training materials do not include specific content for incident response personnel and instead focus on training staff how to report incidents to incident response personnel. UA did not provide any information on its plans or estimated time frames for addressing these deficiencies.

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.

Partially implemented at 24 months—UA has developed policies and procedures requiring its individual units to follow its incident response process; however, these policies and procedures do not include steps for ensuring that the units implement recommendations to address identified noncompliance. UA explained that an incident report is generated at the end of an incident response process, and this report includes the ISO's suggested recommendations to prevent or mitigate future similar incidents. Individual units are responsible for implementing these recommendations, but if they decide not to implement them, the ISO does not take steps to enforce compliance.

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

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;

Implemented at 66 months—ABOR has developed and approved revisions to its policy related to university responsibilities for IT security that require the universities to monitor and annually report on IT security program effectiveness and IT risk assessments to ABOR's Audit and Risk Management committee. Consistent with this policy, the universities presented information on their enterprise risks,

including IT security program effectiveness and risk assessment efforts, to ABOR's Audit and Risk Management committee during its June 2023 meeting. As part of their presentations, the universities reported taking steps to develop strategic IT security program goals and metrics; performing IT audits to assess key IT governance control areas such as access management, change management, and computer operations; and developing automated monitoring and threat-detection controls. The universities also answered committee members' questions about the IT security information presented during the meeting. The universities are scheduled to again provide updates on the implementation and effectiveness of their IT security program goals and metrics to ABOR's Audit and Risk Management committee during its June 2024 meeting.

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

Implemented at 24 months

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

Implemented at 66 months—See explanation for recommendation 5.1a.