MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

ARIZONA AUDITOR GENERAL
LINDSEY A. PERRY

JOSEPH D. MOORE
DEPUTY AUDITOR GENERAL

March 28, 2019

The Honorable Rick Gray, Chair
Joint Legislative Audit Committee

The Honorable Anthony Kern, Vice Chair
Joint Legislative Audit Committee

Dear Senator Gray and Representative Kern:

Our Office has recently completed an initial followup of Arizona's Universities—Information Technology Security regarding the implementation status of the 58 audit recommendations (including sub-parts of the recommendations) presented in the performance audit report released in June 2018 (Auditor General Report 18-104). As the attached grid indicates:

- 11 have been implemented.
- 3 have been partially implemented.
- 35 are in the process of being implemented.
- 3 have not been implemented.
- 6 are not yet applicable.

Our Office will conduct an 18-month followup on the status of those recommendations that have not yet been fully implemented.

Sincerely,
Dale Chapman, Director
Performance Audit Division

cc: John Arnold, Executive 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
University of Arizona

Arizona's Universities—Information Technology Security
Auditor General Report 18-104
Initial Follow-Up Report

Recommendation	Status/Additional Explanation
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.	**Implementation in process** NAU has developed and implemented a security awareness training policy that includes requirements for tracking all employees' security awareness training completion, reporting noncompliance with the training requirement 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. The security awareness training policy also outlines consequences for policy noncompliance. However, as of February 2019, NAU had not developed enforcement procedures for noncompliance with the training requirement or developed an automated tracking system for analyzing all employees' security awareness training completion. NAU reported that it will complete development of and implement enforcement procedures in spring 2019 and estimated that it will implement an automated tracking system by summer 2019.
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**

Recommendation	Status/Additional Explanation
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.	**Implementation in process** As discussed in the performance audit report, UA developed a security awareness training policy in December 2017 that assigned responsibility for ensuring employee compliance with security awareness training to employees' supervisors and identified potential consequences for not completing required training. However, as of February 2019, UA had developed a new draft security awareness training policy intended to replace the existing policy that assigns responsibility for tracking employee compliance with security awareness training to UA's Information Security Office (ISO) and authorizes the ISO and/or UA to take certain actions in instances of policy noncompliance, including limiting network access. Although UA provided evidence that it has the capability to use an automated tracking system for analyzing employees' security awareness training completion, it has not developed written policies and procedures for doing so. Further, it has not developed procedures for following up with or taking corrective action against employees who have not completed required security awareness training. UA estimated that it will complete and implement its draft policy and any associated procedures by December 2019.
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.	**Implementation in process** UA has developed a draft security awareness training policy that requires all employees to complete security awareness training within the first 30 days from their date of hire and to complete a refresher training annually within 60 days of the anniversary of the previous training. In addition, the draft policy assigns UA's ISO the responsibility to define and ensure the implementation of a security awareness training program. However, the policy does not require existing employees to complete security awareness training annually. In addition, the draft policy does not include requirements for periodically evaluating and updating security awareness training materials. UA estimated that it will complete and implement its draft policy and any associated procedures by December 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** ASU revised its vulnerability management policies and procedures to include requirements and guidance for regularly scanning all of the IT systems on its network and its web applications, with specified scanning frequencies based on risk factors, and it has developed and implemented procedures for sharing scan results across the university to help eliminate similar vulnerabilities in other IT systems. In addition, it has developed and begun implementing policies for conducting penetration testing at specified frequencies using a risk-based approach for the IT systems on its network. However, these penetration testing policies do not require all higher-risk web applications to be tested within a specified time frame. ASU has begun implementing the revised policies and procedures, and we will assess the further implementation of this recommendation during the 18-month followup.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** ASU has revised its configuration management policies and procedures to include detailed guidance on configuring IT systems so that these IT systems provide only essential capabilities and prohibit or restrict the use of certain functions, including requirements for developing baseline configurations for some IT systems, defining the frequency of reviews and updates to IT system configurations, and using unique settings when configuring IT resources. ASU has begun implementing the revised policies and procedures, and we will assess the further implementation of this recommendation during the 18-month followup.
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.	**Implementation in process** ASU revised its 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, and it has begun implementing the revised policies and procedures. We will assess the further implementation of this recommendation during the 18-month followup.
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.	**Implementation in process** ASU revised its web application development policies to include requirements for web application developers to use secure coding standards when developing web applications, receive training for developing secure software, and review web application source code and perform security testing before releasing web applications. As of February 2019, ASU had not completed training for all web application developers on developing secure software but estimated that it will complete this training by June 2019.
e. Developing and implementing policies and procedures for protecting system logs from unauthorized access, modification, and deletion.	**Implementation in process** ASU revised its IT security policies to require system logs to be protected from unauthorized access, modification, and deletion. Although it has not developed procedures or other guidance for how its individual units, which are responsible for implementing IT security, should protect system logs, ASU reported that it believes individual unit staff responsible for implementing its log monitoring policies understand how to appropriately protect system logs. We will assess the further implementation of this recommendation during the 18-month followup.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** ASU has developed and begun implementing 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; 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. We will assess the further implementation of this recommendation during the 18-month followup.
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.	**Implementation in process** NAU has revised its vulnerability management policies and procedures to include guidance on risk factors that should be considered for conducting penetration testing of web applications. However, the guidance does not include similar risk factors that should be considered for conducting penetration testing of the IT systems on its network. In addition, NAU has not developed penetration testing policies and procedures that include requirements for conducting penetration testing at specified frequencies based on risk, specify the frequency at which risks will be assessed, outline steps for conducting penetration testing based on identified risks, or include guidance for helping to ensure all higher-risk web applications are tested within a specified time frame. NAU estimated that it will complete development of and implement penetration testing policies and procedures by June 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** NAU has revised its configuration management policies and procedures to require secure baseline configurations, define the frequency of reviews and updates to IT system configurations, and outline requirements for using unique settings when configuring IT resources to limit broad access. However, the revised policies and procedures do not include detailed guidance for how to configure IT systems with only essential capabilities and prohibit or restrict the use of certain functions. NAU estimated that it will complete revisions to and implement its revised policies and procedures by June 2019.
d. Revising its configuration management policies and procedures to indicate that they apply to all NAU IT systems.	**Implementation in process** NAU has developed configuration management policies and procedures that are applicable to all NAU IT systems and estimated that it will implement these policies and procedures by June 2019.
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.	**Implementation in process** NAU has developed additional web application development policies and procedures for using secure coding standards, requiring training for web application developers, and performing security testing before web applications are released. However, these policies and procedures do not include guidance for gathering web application security requirements, conducting threat modeling, and reviewing web application source code for applications developed internally. In addition, NAU has not developed procedures to help ensure that it performs comprehensive security testing before web applications are released. NAU estimated that it will complete and implement its web application development policies and procedures by June 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** NAU has developed and implemented log monitoring policies and procedures that describe the critical IT systems and functions that should be logged, identify who is responsible for ensuring log events are reviewed, require analysis of the logs to identify any patterns that might indicate a potential attack, and outline response actions for specific detected events. Additionally, NAU's Information Technology Services Department, which is responsible for implementing IT security for most of NAU's units, has also developed and implemented a procedure for securely protecting logs. However, NAU's log monitoring policies and procedures do not provide enough guidance for units that are still responsible for implementing their own IT security on how to protect logs. NAU estimated that it will complete and implement its log monitoring policies and procedures by June 2019.
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**

Recommendation	Status/Additional Explanation
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.	**Implementation in process** UA has developed a draft vulnerability and patch management policy that requires scanning and review of scanning results to be performed annually. However, the draft policy does not specify the IT systems and web applications that should be scanned, who should conduct the scanning, or scanning frequencies based on risk factors. In addition, UA has not developed policies or procedures for 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. Further, UA has not developed policies or procedures for conducting penetration testing at specified frequencies based on risk, using a risk-based approach for conducting penetration testing of the IT systems on its network and its web applications, and ensuring all higher-risk web applications are tested within a specified time frame. UA estimated that it will complete and implement its draft vulnerability and patch management policy and any associated procedures by December 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** UA has developed some guidance for configuring IT systems that includes information about how to use unique settings for configuring IT resources in some circumstances. UA reported that it has begun a process to address this recommendation by transitioning the IT systems on its network to third-party cloud-based servers that would include configuration management services. UA estimated that it will complete this project by December 2019.
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.	**Implementation in process** UA has developed a draft vulnerability and patch management policy that requires all patches to be installed as recommended by software manufacturers and/or based on risk. However, the policy does not outline required time frames for installing needed patches. In addition, UA has not developed procedures or other guidance for identifying needed patches, reporting those patches to appropriate individuals responsible for remediation, and applying and testing patches for effectiveness. UA estimated that it will complete and implement its draft vulnerability and patch management policy and any associated procedures by December 2019.
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.	**Implementation in process** UA has developed a draft web application development policy that requires UA's ISO to develop and maintain minimum standards for web application development, administration, and maintenance. However, the draft policy does not require web application developers to be trained on developing secure software, review web application source code before web applications are released, and perform security testing before web applications are released. UA estimated that it will complete development of and implement its draft web application development policy and any associated procedures by December 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** UA has developed a draft log monitoring policy that requires individual units to develop procedures for collecting, monitoring, managing, and reviewing system, application, network, and user logs, including identifying who is responsible for reviewing logs, and time frames for how long logs should be retained. However, the policy does not specify how frequently each log should be monitored or include procedures for analyzing security-related information generated by log monitoring across the university to determine any patterns that might indicate potential attack, nor does it contain requirements for securely protecting logs. UA estimated that it will complete development of and implement its draft log monitoring policy and any associated procedures by December 2019.
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.	**Implementation in process** Although UA has included a policy compliance section in each of its draft IT security policies, the statement does not indicate 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. UA estimated that it will complete and implement its draft policies by December 2019.
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.	**Implementation in process** UA included a statement in each of its draft IT security policies indicating that the policy applies university-wide. Additionally, UA reported that it plans to develop procedures to help guide individual units in implementing its IT security policies. UA estimated that it will complete development of and implement these procedures by December 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** NAU has developed policies that require monitoring the effectiveness of its IT security practices. However, it has not developed procedures for conducting this monitoring. In addition, it has not developed policies and procedures for identifying areas of policy noncompliance and using monitoring results to inform revisions to its IT security policies and procedures. NAU estimated that it will complete and implement its monitoring policies and procedures by June 2019.
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.	**Implementation in process** NAU has developed an information security policy stating that NAU's IT security policies and standards apply to all third parties that have access to NAU's information. In addition, NAU has developed standard terms and conditions related to IT security to be included in contracts with third-party vendors that have access to NAU's data requiring vendors to conduct scanning and penetration testing of their IT systems and security assessments of their processes for protecting data and provide the results of these activities to NAU. Further, the standard terms and conditions authorize NAU to conduct or contract for penetration testing of the third parties' software in some circumstances. However, NAU did not provide documentation demonstrating it has implemented this recommendation. We will assess the further implementation of this recommendation during the 18-month followup.

Recommendation	Status/Additional Explanation
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.	**Not implemented** As of January 2019, UA staff reported that they have begun developing an IT security strategic plan that supports UA's university-wide strategic plan. However, UA did not provide a draft of the IT security strategic plan that is in development. UA estimated that it will complete development of its IT security strategic plan by April 2019.
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.	**Implementation in process** UA has developed a draft policy that outlines some roles and responsibilities related to the management and protection of its IT systems and the data contained in them. For example, the draft policy requires UA's Chief Information Security Officer to develop an information security program and associated policies, assigns individual unit leaders the responsibility for implementing these policies, requires each individual unit to designate a risk manager to manage that unit's information security risks, and specifies that UA's ISO will track policy compliance. However, the draft policy does not describe UA's overall approach for selecting, implementing, and assessing the effectiveness of its IT security controls, and how it will communicate its policies and IT security controls to those responsible for implementing them. UA estimated that it will complete and implement its draft policy and any associated guidance documents by December 2019.
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.	**Not implemented** UA reported that its IT risk assessment process, which it is in the process of revising, will include monitoring for effectiveness of and compliance with its IT security practices and will use results from its annual IT risk assessment process to inform revisions to its policies and procedures. However, as of February 2019, UA's draft procedure for its IT risk assessment process did not include any discussion of or reference to monitoring IT security practices' effectiveness, identifying noncompliance, or using assessment results to inform policy and procedure revisions. UA estimated that it will complete and implement its draft IT risk assessment procedure by December 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** UA has developed standard terms and conditions related to IT security to be included in contracts with third-party vendors that have access to UA's IT systems and data that require vendors to conduct scanning and penetration testing of their IT systems and security assessments of their processes for protecting data and provide the results of these activities to UA upon request. UA is in the process of developing a policy to address IT security in third-party contracts and estimated that it will complete and implement the policy and associated procedures for monitoring and assessing third parties' compliance with the policy by December 2019.
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 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 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, the data owner's identity, 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 planned to implement this recommendation in a different manner by recommending that individual units include IT systems classified as low criticality in their data inventories. Thus, it has revised its policies and procedures to recommend, but not require, individual units to develop data inventories for IT systems classified as low criticality. As a result, ASU cannot ensure that it has a full inventory of 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. The ability to fully implement these policies and procedures would require a complete inventory of web applications classified as low criticality.

Recommendation	Status/Additional Explanation
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 planned to implement this recommendation in a different manner by recommending that individual units include IT systems classified as low criticality in their data inventories. Thus, it has revised its policies and procedures to recommend, but not require, individual units to annually review and update data inventories for IT systems classified as low criticality.
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	**Implementation in process** NAU has begun working with its individual units to educate them on its data classification policies and procedures, including helping them identify the risk levels of information they maintain so that they can appropriately classify data. NAU estimated that its individual units will begin classifying their information and using their data classification results to develop initial data inventories by June 2019. However, NAU has not yet set a deadline by which all individual units must complete the data classification process and develop data inventories.
b. Following up with individual units to ensure they have completed the process.	**Not yet applicable** See explanation for Recommendation 4.4a.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** UA has developed draft policies and procedures that require individual units to develop and update data inventories as part of their IT risk assessments, which they are required to complete at least annually. In addition, UA has developed draft guidance for individual units to use when developing data inventories that state the inventories should include the data's classification level, the data owner's identity, and a brief description of the data classified in data inventories. In November 2018 and February 2019, UA provided training on developing data inventories to individual unit staff who are responsible for overseeing their units' data classification. UA reported that individual units whose staff have completed this training are scheduled to complete IT risk assessments by August 2019, and estimated that it will complete and implement its draft policies and procedures by December 2019.
4.6 UA should:	
a. Establish time frames and guidance for regularly reviewing and updating data inventories; and	**Implementation in process** UA has developed draft policies and procedures that require individual units to develop and update data inventories as part of their IT risk assessments, which they are required to complete at least annually (see explanation for Recommendation 4.5). UA reported that individual units whose staff have completed IT risk assessment training are scheduled to complete IT risk assessments by August 2019.
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.	**Not yet applicable** UA has developed draft policies and procedures that require individual units to develop data inventories (see explanation for Recommendation 4.5), but these policies and procedures have not yet been finalized. Therefore, this recommendation is not yet applicable. UA estimated that it will complete and implement these draft policies and procedures by December 2019.

Recommendation	Status/Additional Explanation
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.	**Implementation in process** NAU has developed 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, and reporting the results to NAU's leadership. The policies and procedures also outline roles and responsibilities for conducting IT risk assessments. NAU completed a university-wide IT risk assessment in fall 2018, including compiling and analyzing the results and identifying corrective actions to manage and address identified risks. However, as of February 2019, NAU reported that it had not fully implemented corrective actions because some of these actions require hiring additional staff, and it had not shared the results with NAU leadership. We will further assess the implementation of this recommendation during the 18-month followup.
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.	**Implementation in process** UA has developed a draft IT risk assessment procedure that provides guidance for managing and addressing identified risks, such as determining risk responses and identifying and choosing controls to protect against identified risks. Between November 2018 and February 2019, UA also provided training on IT risk assessment to individual unit staff who are responsible for overseeing their units' IT risk assessments, and these trainings included sessions on assessing, analyzing, and mitigating IT security risks. However, UA's IT risk assessment policies and procedures do not specify any requirements for managing and addressing identified risks. UA estimated that it will complete and implement its draft IT risk assessment procedure by December 2019
4.9 UA should fully implement its IT risk assessment process by:	
a. Conducting the IT risk assessment in all of its individual units;	**Implementation in process** In November 2018 and February 2019, UA provided training on its IT risk assessment process to individual unit staff who are responsible for overseeing their units' IT risk assessments. UA reported that individual units whose staff have completed this training are scheduled to complete IT risk assessments by August 2019.
b. Compiling and analyzing the results of the IT risk assessment;	**Not yet applicable** UA has not yet conducted an IT risk assessment in all of its units (see explanation for Recommendation 4.9a). Therefore, this recommendation is not yet applicable
c. Using these results to establish a university-wide IT risk profile; and	**Not yet applicable** See explanation for Recommendation 4.9a.

Recommendation	Status/Additional Explanation
d. Communicating the results to UA's leadership.	**Not yet applicable** See explanation for Recommendation 4.9a.
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.	**Implementation in process** NAU has developed incident response policies and procedures for training incident response personnel and testing its incident response process at least annually. NAU reported it plans to conduct formal training for incident response personnel on the new policies and procedures by June 2019.
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.	**Not implemented** Although UA has begun revising its incident response policies and procedures, it has not developed policies and procedures for training incident response personnel and for testing its incident response process. UA reported that it will complete development of policies and procedures for training incident response personnel and for testing its incident response process by May 2019.
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.	**Not yet applicable** UA has not yet completed developing and implementing policies and procedures for training incident response personnel and for testing its incident response process (see explanation for Recommendation 4.11). UA reported that it will develop procedures for assessing whether UA staff are complying with its incident response policies and procedures after it has completed training for incident response personnel and testing its incident response process.
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;	**Implementation in process** ABOR has established a workgroup that includes ABOR, ASU, NAU, and UA staff to revise ABOR's IT security policies. According to ABOR staff, the policy revisions will include developing university monitoring and reporting requirements related to IT security program effectiveness. ABOR staff estimated that the revised policies will be completed by the end of calendar year 2019.

Recommendation	Status/Additional Explanation
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	**Implementation in process** At its January 2019 meeting, ABOR's audit committee approved revisions to each university's respective internal audit department charter requiring their annual audit plans to include components of IT Security, unless otherwise directed by the audit committee. We will assess the universities' implementation of this requirement during our 18-month followup.
c. Reviewing the results of the universities' IT risk assessments.	**Implementation in process** ABOR has established a workgroup that includes ABOR, ASU, NAU, and UA staff to revise ABOR's IT security policies. ABOR staff reported that the revised policies will require the universities to share IT risk assessment results with their respective internal audit departments as part of their university-wide risk assessments, which inform development of the universities' annual internal audit plans. ABOR staff estimated that the revised policies will be completed by the end of calendar year 2019. According to ABOR staff, until ABOR completes and implements its revised policies, it will require the universities to submit status reports on their respective plans to implement IT risk assessment processes.