Arizona Department of Economic Security
Information Technology Security
42-Month Follow-Up Report

The April 2017 Arizona Department of Economic Security—Information Technology Security performance audit report found that the Department should improve security processes and controls over its information technology systems and data, and establish an information security program. The Department's status in implementing the recommendations is as follows:

Status of 34 recommendations

Implemented:	11
In process of being implemented:	22
Not implemented:	**1**

Our Office will continue to follow up with the Department on the status of those recommendations that have not yet been fully implemented as we conduct our work at the Department for the State's financial statement audit.

Finding 1: Department should improve security processes and controls over its IT systems and data

1.1 To help ensure vulnerabilities are effectively identified and addressed, the Department should develop and implement written policies and procedures establishing a formal vulnerability management process. Specifically, as part of its vulnerability management process, the Department should:

a. Ensure that regular vulnerability scanning occurs and is comprehensive, meaning that it includes all systems. To do so, the Department will need to develop and implement procedures for identifying and creating an inventory of all systems, such as with automated tools or software.

Implementation in process—As indicated in our 24-month followup, the Department has developed and implemented a written vulnerability scanning and remediation policy establishing a formal vulnerability management process that includes comprehensive vulnerability scans twice a month. However, the Department reported that it is still identifying and creating an inventory of its systems to ensure that all systems are scanned. The Department did not provide a date for finalizing this inventory and fully implementing this recommendation. The Department plans to finalize this inventory and fully implement this recommendation by July 2021.

b. Include regular, comprehensive vulnerability and penetration testing. If the Department chooses to continue using contractors to perform this work, it should ensure its contractors effectively identify vulnerabilities by conducting more frequent, comprehensive testing. If the Department will primarily rely on using internal staff for vulnerability and penetration testing, the Department will need to develop inhouse expertise on vulnerability and penetration testing, including common attack strategies currently used by hackers. For example, in addition to formal training, widely used IT security sources, such as IT security conferences and blogs, contain information on the newest attack methods and defenses.

Implemented at 24 months

c. Include a well-defined remediation process. This process should identify the specific staff responsible for addressing identified vulnerabilities, including the number and type of staff involved; specify staff roles

and responsibilities related to reviewing and addressing detected vulnerabilities or formally accepting their associated risks; and set specific time frames for completing the remediation process.

Implementation in process—The Department has developed a written vulnerability scanning and remediation plan that includes a well-defined remediation process. However, the Department indicated that it is still in the process of implementing its remediation process and plans to fully do so by February 2021.

d. Train appropriate staff on the vulnerability management process and the supporting policies and procedures.

Implemented at 42 months

1.2 The Department should continue to implement written patch management policies and procedures to guide its staff and efforts in this area. These written policies and procedures should include the following:

a. Identifying and determining the updates that are available and whether a software or system update should be applied, including testing and documenting the effectiveness and potential side effects of available patches before installation;

Implemented at 24 months

b. Applying available patches in a timely manner and reviewing the updates to ensure they are effectively applied; and

Implementation in process—The Department has written patch management procedures that include time frames for testing and applying patches to help ensure that patches are applied in a timely and effective manner. However, during this followup, the Department indicated that it recently hired additional personnel to coordinate and assist in its systems' patching. The Department also indicated that it plans to implement this recommendation by July 2021.

c. Accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances, such as older applications that may not be able to run or will not perform properly with the updates applied.

Implementation in process—As indicated in our 24-month followup, the Department has written patch management procedures that include accepting, justifying, and documenting the risk of not updating the software or system if there are extenuating circumstances. However, during this followup, the Department indicated that it recently hired additional personnel who will coordinate and assist in system patching. The Department expects to implement this recommendation by July 2021.

1.3 The Department should continue its efforts to develop and implement written policies and procedures for securely configuring its IT systems. These policies and procedures should include requirements for:

a. Configuring the Department's IT systems so that they do not provide more functionality than is necessary, including provisions and controls to ensure that baseline configurations, which provide an agreed-upon set of attributes that serve as a basis for information system settings, are developed and documented for each IT system, as appropriate;

Implementation in process—Although the Department has updated its written policy and procedures for securely configuring its IT systems so that the systems do not provide more functionality than is necessary, the Department has not yet established baseline configurations for its systems. The Department indicated that it is in the process of developing its configuration management database inventory and will implement its configuration procedures after this inventory is completed. The Department reported that it expects to implement this recommendation by January 2021.

b. Developing and documenting specific configuration settings;

Implementation in process—Although the Department has updated its written policy and procedures for developing and documenting specific configuration settings, and has established specific configuration settings, it has not done so for all systems. In addition, as stated in the explanation for Recommendation 1.3a, the Department is in the process of developing its configuration management database inventory and

will implement its configuration procedures after this inventory is completed. The Department reported that it expects to implement this recommendation by January 2021.

c. Ensuring unique or randomized settings are used for critical functionality; and

Implementation in process—Although the Department has updated its policies and procedures to address unique settings, they do not include requirements for ensuring randomized settings are used for critical functionality. The Department reported that it plans to implement this recommendation by January 2021.

d. Defining the frequency of reviews and of updates to configurations.

Implementation in process—The Department's updated policy and procedures for securely configuring systems define the frequency of review and of updates to configurations. However, the Department has yet to establish baseline configurations for its systems and until it does so, cannot review or update them. The Department reported that it plans to establish baseline configurations and implement this policy and procedure by January 2021.

1.4 To ensure the access-removal process is properly conducted, the Department should develop and implement written policies and procedures for:

a. Reviewing and adjusting, as needed, user access and account access privileges periodically, and ensure that accounts for terminated employees are disabled or removed as soon after the employee leaves as is practical.

Implementation in process—As indicated in our 24-month followup, the Department has developed an information systems access control policy and associated procedures that require managers to immediately notify IT security analysts when employees are terminated. However, the Department reported that these notifications are made manually, and it plans to replace these procedures with an account identity and access management system (IAM) that will automate the removal or disabling of account access when employees are terminated. The Department estimated it will implement the IAM by December 2021.

b. Establishing requirements and time frames for changing service account passwords, and ensure that all passwords are changed in accordance with its policies.

Implementation in process—The Department has updated its procedures for establishing requirements and time frames for changing service account passwords, and its policy requires these passwords to be changed when an individual who has access to the account leaves the agency or loses access to the system for which the service account is used. However, as indicated in the explanation for Recommendation 1.4a, the Department reported that it plans to move to an IAM, which will help it define and manage access and passwords according to its policies and procedures. The Department reported that it plans to fully implement this recommendation by December 2021.

1.5 The Department should develop and implement a continuous log-monitoring program that includes written policies and procedures for monitoring critical IT activities. The Department's policies and procedures should:

a. Describe the IT systems and functions within each IT system that should be logged;

Implementation in process—Although the Department has begun developing system-specific logging procedures, its procedures do not yet define the specific functions within each system that should be logged. As of July 2020, the Department had begun using a new log-monitoring system and reported that it plans to configure the new system to include system-specific functions that should be logged. The Department estimated that it will fully implement the new log-monitoring system by the end of March 2021.

b. Specify how frequently each log should be monitored;

Implementation in process—The Department's system security audit policies and procedures specify how frequently each log should be monitored, who is responsible for ensuring log events are captured and reviewed, the requirements for securely protecting the logs, and the time frames for retaining logs before they are deleted. However, as of July 2020, the Department changed from using a vendor for this process to using a new in-house log-monitoring system. The Department reported that its security staff continuously

monitor logs generated by the new system, that its system will also send alerts for events that the Department deems critical to applicable Department staff for review on a regular basis, and that it plans to move logs onto a separate encrypted backup server in order to securely protect and retain them. The Department needs to update its policies and procedures once it has fully established its new processes and reported that it will fully implement the new log-monitoring system by the end of March 2021.

c. Identify who is responsible for ensuring log events are captured and reviewing log events on a regular basis;

Implementation in process—See explanation for Recommendation 1.5b.

d. Develop standard response actions that should be taken for detected events, including informing designated personnel of security risks to the Department and for individual information systems; and

Implemented at 42 months

e. Include requirements for securely protecting the logs and time frames for how long the logs should be retained before being deleted.

Implementation in process—See explanation for Recommendation 1.5b.

1.6 The Department should develop and implement written policies and procedures for developing, securing, and testing web-based applications. The Department's policies and procedures should include the following:

a. Gathering security requirements;

Not implemented—In March 2020, the Department revised its web application development policy and procedures. However, the revisions do not address all the required components for gathering security requirements, such as describing the functionality of the security controls. This would include ensuring the availability of web application data and that the web application and its data are classified and protected based on its level of risk.

b. Up-to-date secure coding standards or conventions;

Implemented at 42 months

c. Threat modeling during development;

Implementation in process—The Department's revised web application development policy and procedures do not include important threat modeling details we identified and shared with the Department during our 24-month followup, including developing potential scenarios (use-cases) to understand how the web applications might be used and methods for identifying security threats to them. The Department reported that it has begun using a new tool for performing threat modeling and has trained its developers on how to use the tool and plans to update its policies and procedures and implement this recommendation by January 2021.

d. Source code review; and

Implemented at 42 months

e. Security testing before releasing a web-based application to the live environment.

Implementation in process—As indicated in our 24-month followup, the Department had developed procedures for performing security testing before releasing a web application to the live environment. However, the Department indicated that it still needs to procure security testing tools and train staff to use the tools it acquires. The Department reported that it plans to implement this recommendation by March 2021.

Finding 2: Department should establish an information security program

2.1 To help ensure the Department's IT systems and data are sufficiently protected, the Department should establish a written plan for developing and implementing a Department-wide information security program. The Department's plan should establish the specific tasks required to develop and implement an information security program, time frames for completion, and persons responsible for completing the specific tasks.

Implementation in process—The Department has established a written plan for developing and implementing a Department-wide information security program. The plan establishes the specific tasks required to develop and implement an information security program and persons responsible for completing the specific tasks. Although the Department has established time frames for several tasks in the plan, it indicated it has yet to implement its plan Department-wide but plans to do so by June 2021.

2.2 The Department's written plan for developing and implementing a Department-wide information security program should include the following tasks:

a. Developing and implementing Department-wide IT risk assessment procedures that are consistent with ASET requirements and best practices, regularly perform Department-wide IT risk assessments, document the results and potential impacts of the identified risks, and use the risk assessment results to prioritize its information security program efforts and address identified risks.

Implementation in process—The Department has developed Department-wide IT risk assessment procedures that are consistent with ASET requirements and industry standards and has developed a risk management plan that provides additional guidance on the risk assessment process. However, the Department has yet to perform a Department-wide IT risk assessment and reported that it plans to do so by July 2021.

b. Further defining information security program authority, roles, and responsibilities, including strengthening the CISO's authority to monitor and ensure compliance with the program by including this responsibility in its information security program policy, and ensuring the roles and responsibilities of any other security staff who will be involved in implementing the information security program are clearly defined in its information security program policy.

Implemented at 42 months

c. Establishing an IT security workforce development strategy consistent with best practices, such as defining the knowledge and skill levels needed to perform job duties, conducting role-based training programs, and defining standards for measuring and building individual qualifications for employees with IT security-related positions.

Implemented at 42 months

d. Assessing its resources, such as staffing levels and the budget needed to implement the information security program, and ensuring that resources are available as needed. For example, the Department should ensure that its current resources are being used effectively and efficiently and should develop a process to ensure it will have sufficient resources to implement and run the information security program. In addition, the Department should analyze the number and type of staffing needed to implement an information security program and ensure it has adequate staff, whether through reassigning staff, contracting for additional services, or other means.

Implementation in process—Although the Department has defined the roles necessary to implement an information security program, it has not assessed whether it is efficiently and effectively using its current resources or what staffing and budget resources it will need to implement its program. The Department reported that it plans to fully implement this recommendation by August 2021.

e. Establishing a method for regularly communicating the authority, roles, and responsibilities for the information security program to Department staff.

Implemented at 42 months

Finding 3: Department should enhance efforts to establish information security policies and procedures

3.1 The Department should ensure that it further develops and implements information security policies and procedures consistent with ASET requirements for the areas of data classification, incident response, and information security awareness education and training. Specifically, the Department should:

a. Develop and implement procedures for its data classification process that are consistent with ASET requirements, such as protecting the data based on its level of risk; for example, whether the data is confidential; and developing a data classification inventory that is updated regularly;

Implementation in process—As reported in our 24-month followup, the Department updated its data classification policy and corresponding procedure to be consistent with ASET requirements. However, as of July 2020, the Department had yet to start the process of classifying its data or developing a data classification inventory but reported that it plans to do so by June 2021.

b. Enhance its incident-response-planning policy to include an information spillage response, identify roles and responsibilities for the incident response process, and provide responding individuals with the authority to make critical decisions;

Implemented at 24 months

c. Develop and approve a comprehensive incident response plan and associated procedures related to incident response training, testing, and monitoring; and

Implementation in process—The Department has developed and implemented a comprehensive incident response plan and associated procedures related to incident response training and monitoring consistent with ASET requirements. However, the Department indicated it has not tested its incident response plan and will do so by December 2020.

d. Improve its information security awareness training and education program and procedures to ensure they are effective and consistent with ASET requirements and best practices, such as implementing role-based training based on users' job duties and training for employees to recognize and report malicious activities internal to the Department. This training should inform users about common methods used by attackers, such as phishing emails and practical examples of phishing attacks to foster a more security-focused culture within the Department. In addition, the Department should simulate attacks to test the training's effectiveness and provide additional training to individuals who do not appropriately respond to simulated attacks.

Implementation in process—The Department has developed and implemented security awareness policies and procedures consistent with ASET requirements that require annual security awareness training for all employees to recognize and report malicious activities internal to the Department. However, auditors found that from May 2019 to May 2020, only 53 percent of the Department's employees had taken the required annual security awareness training. In addition, although the Department simulates attacks to test the training's effectiveness, it does not provide additional training to individuals who do not appropriately respond to simulated attacks. Further, the Department indicated that although it provides informal role-based training for some security roles, it had not fully implemented role-based security training based on users' job duties. The Department reported that it plans to fully implement this recommendation by July 2021.

3.2 As the Department creates its written plan for developing and implementing an information security program (see Finding 2, pages 15 through 19), it should ensure that its written plan includes a process for adequately developing and implementing all ASET-required policies and procedures. This process should include documenting time frames for completing key steps such as developing each written procedure and specifying persons responsible for completing specific tasks, such as developing the procedures, reviewing them to ensure consistency with ASET requirements and best practices, and approving the policies and procedures.

Implemented at 42 months