



DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

June 4, 2014

The Honorable John Allen, Chair
Joint Legislative Audit Committee

The Honorable Chester Crandell, Vice Chair
Joint Legislative Audit Committee

Dear Representative Allen and Senator Crandell:

Our Office has recently completed an 18-month followup of the Arizona Department of Administration (Department) State Data Center regarding the implementation status of 37 audit recommendations (including sub-parts of the recommendations) presented in the IT procedural review report released in August 2012. As the attached grid indicates:

- 18 have been implemented, and
- 19 are in the process of being implemented.

Unless otherwise directed by the Joint Legislative Audit Committee, our Office will conduct a 36-month followup with the Department on the status of those recommendations that have not yet been fully implemented

Sincerely,

Joseph D. Moore, Director
Information Technology Services Division

Attachment

cc: Brian C. McNeil, Director
Arizona Department of Administration

Arizona Department of Administration— State Data Center IT Procedural Review 18 Month Follow-Up Report

Recommendation	Status/Additional Explanation
----------------	-------------------------------

Chapter 1: Data Management Issues

1.1 Disaster Recovery Plans and Delineation of Related Responsibilities Are Incomplete

A. The Department should:

a. Create and finalize a comprehensive disaster recovery plan, which includes all system and infrastructure components for which it is responsible, and addresses important elements such as regulatory and contractual requirements, the Department's overall business continuity needs, IT resource management requirements and interdependencies, an analysis of business impacts, risk assessments, emergency procedures, testing, and ongoing maintenance of its disaster recovery efforts.

Implemented at 18 months

b. Formally document and publish the plan. The plan should include information related to the activation and notification, recovery, and reconstitution phases, and should include supporting documentation.

Implemented at 18 months

c. Test the plan on a regular basis using realistic scenarios, as defined in the plan, and document and make modifications when necessary to correct any problems identified through testing.

Implemented at 18 months

B. The Data Center should establish formal procedures and benchmarks to ensure that customers who contract with it for disaster recovery services receive the services in accordance with agreed-upon benchmarks and service guarantees. The procedures should ensure that customers' systems are appropriately identified, listed, prioritized, and handled in accordance with relative importance.

Implementation in process

The Department has begun the process of prioritizing customer systems by creating a business impact matrix, which currently includes its largest customers. The Department is still establishing formal procedures and benchmarks, including finalizing the matrix for all customers and standardizing contract language to describe all services offered clearly.

C. The Data Center should better publicize to its open systems customers the services it provides to them and clarify the roles and responsibilities that it and its customers play in disaster recovery efforts. This information should be included in contracts for services and provided in summary form to the appropriately responsible individual at the customer organization.

Implementation in process

The Department is reorganizing contract wording to improve the clarity and readability of all Data Center service contracts. The Department is also in the process of developing a summary document of provided services to inform all customers of the available services.

1.2 Data Center Does Not Have Sufficient Process for Identifying High-Risk Assets

The Data Center should establish, implement, and maintain a formal inventory and a documented process for identifying and categorizing its organization-critical and high-risk assets. The IT inventory should contain information on applications, data, hardware, software, network resources and services, and facilities; and should assign corresponding security risk ratings to these assets.

Implemented at 18 months

1.3 Lack of Well-Established Data Classification Program Could Affect Ability to Prevent Unauthorized Access, Modification, Disclosure, or Destruction of Sensitive Data

To help ensure that sensitive data is properly protected, the Department should:

- A. Complete its development, review, and implementation of a documented organization-wide data classification policy and process.

Implementation in process

The Department implemented a new policy as of January 1, 2014, regarding data classification; however, it is still developing standard procedures for data classification efforts. Following the development of these procedures, the Department is planning to train its staff regarding data classification starting in May 2014. The Department indicated it plans to start the process of classifying its data after the training is complete.

- B. Ensure that its process is based on risks and requirements, such as confidentiality and sensitivity of the information, consisting of an inventory of information classification details that includes assigned classification, identity of the information owner, and a brief description of information classified; and that it is communicated to all affected parties, reviewed, and updated regularly.

Implementation in process

The Department is in the process of developing a template to store required data classification details. This template will guide staff on how to document department data.

Chapter 2: Security Issues

2.1 Lack of Risk Assessment Process Could Hinder Ability to Protect Sensitive Information or Critical Infrastructure

The Department should establish and implement a process for performing risk assessments that assigns responsibility, mandates regular assessments, contains a structured methodology for assessing risks, documents results and potential impact of results, uses results to make changes to the organization's security program, and reports results to top management. Additionally, the Department should perform risk assessments on an annual schedule or as significant changes are made to information resources as outlined in its current policy.

Implementation in Process

The Department has created a new policy that includes requirements for developing risk assessments for each of its divisions. These risk assessments are required to occur annually. The Department's ASET division has fully implemented this policy and has created a risk assessment document. The Department indicated that the remaining divisions would be educated on the policy between May and July 2014, with the new policy anticipated to be in effect department-wide in August 2014.

2.2 Data Center Does Not Have Effective Process or Enforcement Mechanism for Communicating About and Ensuring Security Compliance

The Department should establish and implement a formal security compliance process, which consists of obtaining regular confirmation of compliance from process owners, ensuring that internal and external compliance reviews are performed against internal policies, and implementing a process to monitor and report on noncompliance issues. As a component of its compliance process, the Department should include an enforcement mechanism to ensure that policies are effective and are being followed.

Implementation in process

The Department has begun using several tools to evaluate security compliance. The Department is still configuring compliance reviews and developing repeatable processes to ensure these tools are evaluating compliance with relevant internal policies.

2.3 Computer Security Awareness Training Policies and Requirements Not Being Met

A. The Department should enhance its policy related to security awareness training to include adequate guidance on what should be included in such training—and training materials—being sure to address all areas required by state policy; and should develop mechanisms to ensure that the policy is being followed by all of its Business Units.

Implemented at 18 months

B. As required by state policy, the Department should establish a department-wide security awareness education and training program. The program should:

Implemented at 18 months

a. Be designed to ensure that employees understand relevant IT security risks and threats, the Department's IT-related security policies, and each individual's role in carrying out those policies.

Implemented at 18 months

Recommendation	Status/Additional Explanation
b. Incorporate a mechanism to periodically evaluate the program's effectiveness and make changes to it as necessary.	Implemented at 18 months
c. Consider and address the type and form of training needed relevant to staff members' roles and functions.	Implemented at 18 months
d. Be provided annually, or upon occurrence of a specific event, such as a change in job responsibilities or employment status.	Implemented at 18 months

2.4 Although Steps Have Been Taken to Protect Networks and Resources, More Could Be Done to Further Limit Access and Identify and Mitigate Vulnerabilities

The Department should:

A. Ensure that security policies are followed and security mechanisms are in use for all applications and systems.	<p>Implementation in process</p> <p>The Department has implemented security mechanisms for applications and systems and has created new security policies to dictate best practices for securing systems. The Department indicated it is in the process of implementing these policies in all divisions.</p>
B. Review the configuration of its servers to ensure that only needed services are running, that services and associated user and system accounts are configured securely, and that critical services are segmented from those available through the public network.	<p>Implementation in process</p> <p>The Department has created baseline configurations and procedures for new systems; however, the Department is in the process of reviewing server configurations on current systems. Specifically, the Department is still reviewing pre-existing servers' user and system accounts to ensure they are appropriate.</p>
C. Use its network vulnerability scanning software or perform other procedures to regularly test all segments of its network, identify potential vulnerabilities, and mitigate them to the extent possible.	Implemented at 18 months
D. Develop and implement a configuration management policy that covers its IT resources and addresses security considerations.	<p>Implementation in process</p> <p>ADOA-ASET has developed a process for configuration management, but is still drafting and approving written policies and procedures for configuration management department-wide. The Department indicated that once the policies and procedures are approved, it would begin implementation department-wide.</p>

Recommendation**Status/Additional Explanation****2.5 Weaknesses in IT Security Incident Management May Result In Inconsistent and Ineffective Incident Response**

The Department should complete, approve, and implement an organization-wide policy and process for incident response management. It should ensure that all the appropriate Business Units are involved and that the policies and procedures identify roles and responsibilities over incident handling provide responding individuals with a clear plan and authority to make critical decisions, and provide information on how to identify, respond to, recover from, and follow up on incidents.

Implementation in process

ADOA-ASET has developed and implemented an Incident Response Planning Policy, effective January 1, 2014. The Department indicated it is still developing standards and procedures to guide its incident response efforts department-wide.

2.6 Failure to Monitor Security Logs Prevents Department From Being Able to Effectively Identify Unauthorized System Activity and Attempts to Circumvent Controls

A. The Data Center should develop and implement log management policies and procedures. Those procedures should ensure that all important system, application, and security-related events be defined and recorded in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis.

Implementation in Process

The Department has implemented a policy that includes guidance on log management activities; however, the Department indicated it is still developing procedures, which would include details on identifying which activities to review and how to investigate those activities.

B. The Department should establish and implement formalized procedures to ensure that audit logs are regularly reviewed for critical events and that any unauthorized activity detected is investigated and addressed in a timely manner.

Implementation in process

See 2.6A above.

Chapter 3: Identity and User Account Management Issues**3.1 Department's Use of Generic Accounts and Ineffective Policies Undermine User Control and Accountability**

A. The Department should ensure that all of its Business Units are adhering to the Data Center's Access Control Policy, which provides guidance on: a) ensuring all user accounts are uniquely identifiable and assigned to an individual employee; and b) periodically reviewing all user access lists to ensure that they are still needed, establish user identification, and enforce access rights appropriate to the person's job duties and responsibilities.

Implementation in process

The Department has created and implemented a policy regarding user accounts. This policy requires unique user accounts for individual employees and regular reviews. The Department has implemented processes for reviewing some systems, but is still developing processes for reviewing users of the remaining department systems.

Recommendation	Status/Additional Explanation
<p>B. The Department should review the use of generic user accounts and should eliminate ones that are no longer needed and implement procedures to better monitor ones that are retained.</p>	<p>Implementation in process The Department has created and implemented a policy regarding user accounts. This policy requires the elimination of all generic accounts except for those explicitly required for proper system functionality. The Department has implemented processes for reviewing some systems, but is still developing processes for reviewing generic accounts of the remaining department systems.</p>

3.2 Policies on Terminated Employees Not Consistently Followed, Increasing Risk of Theft, Manipulation, or Misuse of Systems and Data

The Department should:

<p>A. Ensure that all of its Business Units are adhering to the Access Control Policy by removing user accounts when an employee is no longer employed, and regularly reviewing access lists to identify changes needing such action.</p>	<p>Implementation in process See explanation 3.1A above.</p>
<p>B. Determine what problems exist with the system used to inactivate network employee accounts based on pay status and correct them, or develop alternate procedures to ensure that proper action is taken.</p>	<p>Implemented at 6 months</p>

3.3 Inadequate Documentation Makes It Difficult to Confirm User Access Has Been Properly Authorized and Is Appropriate

<p>A. The Department should take steps to ensure that it maintains required authorization documentation on file for all new account creation requests as outlined in its policy.</p>	<p>Implemented at 18 months</p>
<p>B. Management should regularly conduct a review of a sample of user accounts to ensure compliance with its policy.</p>	<p>Implementation in process See explanation 3.1A above.</p>

Chapter 4: Change and Configuration Management Issues

4.1 Data Center Lacks Formal Change Management Process

The Data Center should:

<p>A. Complete development of change management policies procedures, to include:</p>	<p>Implemented at 6 months</p>
--	---------------------------------------

Recommendation	Status/Additional Explanation
----------------	-------------------------------

- a. Roles and responsibilities;
- b. Classification and prioritization of all changes based on business risk;
- c. Assessment of impact;
- d. Authorization and approval of all changes by the business process owners and IT;
- e. Testing plans;
- f. Tracking and status of changes;
- g. Impact on data integrity;
- h. Emergency changes;
- i. Tracking, status and reporting of changes; and
- j. Change closure.

B. Require the Change Control Form to be completed consistently and maintained for all changes, and to be updated to include all necessary items, such as impact analysis and testing plans.	Implemented at 18 months
--	---------------------------------

C. Consistently maintain all relevant documentation for each change in a central repository or location.	Implemented at 18 months
--	---------------------------------

D. Review the change control process in use by the Enterprise Infrastructure and Communications (EIC) Office and consider its applicability to the Data Center's broader IT requirements. If deemed appropriate, consider incorporation of relevant EIC practices into the Data Center's existing process.	Implemented at 6 months
--	--------------------------------

4.2 Data Center Does Not Have a Required Formal, Defined Configuration Management Process

The Data Center should develop and implement a documented, organization-wide configuration management process that is in-line with IT standard best practice and state requirements. The process should include defined responsibilities, consistent identification of configurations of IT devices, network components, documented change control, tracking of configuration items, and periodic review of configurations.

Implementation in process

The Department is in the process of implementing a full configuration management database. The Department indicated it is working with an outside vendor to configure and implement the system.

Chapter 5: Policies and Procedures Issues

5.1 Data Center is Either Missing or Has Ineffective Policies Over a Number of Significant Areas and Lacks An Effective Enforcement Mechanism

The Department should:

A. Perform a comprehensive review of its IT policies and procedures, comparing them against state-wide standards and IT best practices to 1) identify missing items, and 2) items that are incomplete, out of date, or not in use.	Implemented at 18 months
--	---------------------------------

Recommendation**Status/Additional Explanation**

B. Prioritize the results from its review and develop and implement, where necessary, effective IT policies and procedures that align with business requirements and then monitor for compliance with its policies and procedures.

Implementation in process

The Department has reviewed its policies and updated them to better align with current standards and methods of operation; however, it is still implementing some policies and procedures. In addition, the Department is still developing methods for monitoring compliance with its new IT policies.

C. Develop a strategy that ensures that IT policies and procedures are effectively and consistently communicated and disseminated to all affected parties within the Department.

Implementation in process

The Department has approved all newly developed policies and has communicated them to management. The Department is still determining where to store the policies to be easily accessible by all staff and is developing trainings to inform all staff of policy changes and strategies to implement these practices.