STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-187
March 2018

AGENCY FOR STATE TECHNOLOGY

State Data Center Operations



Sherrill F. Norman, CPA
Auditor General

Executive Director of the Agency for State Technology

Section 20.61, Florida Statutes, creates the Agency for State Technology. The head of the Agency is the Executive Director and the State's Chief Information Officer who is appointed by the Governor, subject to confirmation by the Senate. During the period of our audit, Jason M. Allison served as Executive Director and Chief Information Officer through March 7, 2017, and Eric Larson was appointed by the Governor on March 10, 2017, and confirmed by the Senate on February 6, 2018.

The team leader was Andrew Denny, CISA, and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

AGENCY FOR STATE TECHNOLOGY

State Data Center Operations

SUMMARY

This operational audit of the Agency for State Technology (AST) focused on evaluating selected information technology (IT) controls applicable to State Data Center operations and included a follow-up on the findings included in our report No. 2017-087. Our audit disclosed the following:

Finding 1: The State Data Center's disaster recovery plan and annual testing continue to need improvement to ensure that critical State Data Center operations are recovered and continue in the event of a disaster or other interruption in service.

Finding 2: The State Data Center's continuity of operations plan and testing continue to need improvement to ensure the timely resumption of critical business operations in the event of a disaster or other interruption in service.

Finding 3: AST management had not defined the repositories for the inventory of IT resources at the State Data Center and the inventories maintained were not complete and, in some cases were not accurate, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated to ensure the timely implementation of the latest security patches and other critical updates from IT vendors.

Finding 4: AST policies, procedures, and processes for reconciling and tracking backup tapes need improvement to ensure all backup tapes are accounted for and location and status records are accurate.

Finding 5: Some access privileges did not promote an appropriate separation of duties or were not necessary based on the user's assigned job duties.

Finding 6: The AST lacked a policy for comprehensive periodic access reviews and the various AST Bureau procedures for the performance and documentation of access reviews need improvement to ensure assigned access remains appropriate.

Finding 7: State Data Center backup controls continue to need improvement to ensure backups for all IT resources requiring backup are appropriately performed and customer data is readily recoverable in response to an unexpected event.

Finding 8: The AST lacked policies and procedures for the management and monitoring of software licensing agreements. Such policies and procedures help prevent software licensing violations.

Finding 9: The State Data Center's monitoring and reporting of the performance metrics for database services provided to customer entities, as defined in service-level agreements, need improvement to ensure that critical incidents affecting the database services are timely detected, documented, and, as applicable, resolved.

Finding 10: The AST's Computer Incident Response Team processes need enhancement to promote prompt and appropriate responses to cybersecurity events.

Finding 11: Certain State Data Center security controls related to tape encryption, vulnerability management, configuration management, user authentication, shared accounts, service accounts, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of State Data Center customer entity data and related IT resources.

BACKGROUND

The Agency for State Technology (AST) was established on July 1, 2014, by the Legislature and the Executive Director of the AST is the State's Chief Information Officer. Pursuant to State law,[1] AST powers, duties, and functions include, among other things, developing and publishing information technology (IT) policy for the management of the State's IT resources, overseeing the State's essential technology projects, and managing the State Data Center (SDC).

According to State law,[2] the SDC's duties are to:

- Offer, develop, and support services and applications defined in service-level agreements executed with its customer entities.
- Maintain performance of the SDC by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity.
- Develop and implement a business continuity plan and a disaster recovery plan, and beginning July 1, 2015, and annually thereafter, conduct a live exercise of the plan.
- Enter into a service-level agreement with each customer entity to provide the required type and level of service or services.
- Be the custodian of resources and equipment located in and operated, supported, and managed by the SDC.
- Assume administrative access rights to resources and equipment, including servers, network components, and other devices consolidated into the SDC.

As shown in ***EXHIBIT A*** to this report, as of December 31, 2017, the SDC provided IT services to 32 customer entities consisting of State agencies, municipal and county governments, a judicial branch entity, special districts, and other governmental entities as well as nonprofit entities that contract with the SDC for IT services. The SDC provides to its customer entities IT services covering a variety of services and computing environments, including data center facilities and operations, mainframe platforms, network platforms, open systems platforms, storage platforms, backup and recovery platforms, database platforms, Windows platforms, managed applications, and optional custom offerings.

[1] Section 282.0051, Florida Statutes.

[2] Section 282.201, Florida Statutes.

FINDINGS AND RECOMMENDATIONS

Finding 1: Disaster Recovery Planning

Disaster recovery planning is intended to facilitate the timely recovery of key applications, data, and services in the event of a disaster or other interruption of service. According to State law,[3] the Legislature intends that the most efficient and effective means of providing quality utility data processing services to State agencies requires that computing resources be concentrated in quality facilities that provide the proper security, disaster recovery, infrastructure, and staff resources to ensure that the State's data is maintained reliably and safely, and is recoverable in the event of a disaster. State law[4] requires the SDC to, among other things, develop and implement a Disaster Recovery Plan (DRP), and beginning July 1, 2015, and annually thereafter, conduct a live exercise of the DRP. Additionally, State law[5] requires the SDC to maintain performance of the SDC by ensuring proper data backup, data backup recovery, disaster recovery, and appropriate security, power, cooling, fire suppression, and capacity.

Our audit procedures disclosed that, while the AST had created a DRP as of May 5, 2017, the AST DRP did not contain sufficiently detailed instructions for recoverability of the SDC infrastructure. In response to our audit inquiry, AST management provided a document with detailed instructions for recoverability for 1 of the 21 critical applications at the SDC; however, the instructions document was not referenced in either the DRP or the *Disaster Recovery Test 2016-17 Final Report*. Also, the AST did not identify the IT components supporting all critical applications identified in the AST DRP. Specifically, the AST DRP did not include the required IT resources supporting:

- The Data Protection Advisor.
- The Security Incident Event Manager (SIEM). In response to our audit inquiry, AST management stated that the SIEM had been misclassified as a critical application.
- Audit logging.

Additionally, as of November 6, 2017, the AST had not conducted a full live exercise of the AST DRP. While the AST scheduled an initial test of the AST DRP at the SDC disaster recovery site over 5 days (June 19, 2017, through June 23, 2017), the AST only tested the AST DRP for 50 minutes on June 19, 2017, and the testing only included the recovery of 11 of the 21 critical applications identified in the AST DRP. In response to our audit inquiry, AST management indicated that they classified and prioritized applications to include in the scope of the DRP testing and a business decision was made to include 11 applications in the initial round of DRP testing. However, our review of the AST DRP testing disclosed that 3 of the 11 applications identified for testing were not included in the 11 applications tested on June 19, 2017.

Also, we reviewed the *Disaster Recovery Test 2016-17 Final Report* for results of successful recovery and found that the report lacked both appropriately detailed instructions followed for recovery and the

[3] Section 282.201(1), Florida Statutes.

[4] Section 282.201(2)(c), Florida Statutes.

[5] Section 282.201(2)(b), Florida Statutes.

detailed results of testing. As a result, AST records did not demonstrate that the testing for the 11 applications was appropriately completed.

Absent the development of a comprehensive AST DRP and full disaster recovery testing that includes critical SDC applications and documents the instructions followed and the detailed results, the risk is increased that critical SDC applications will not be timely and orderly resumed in the event of a disaster or other interruption of service. A similar issue was noted in our report No. 2017-087.

Recommendation: To ensure recoverability of the critical SDC applications in the event of a disaster or other interruption of service, we again recommend that AST management continue development and implementation of a comprehensive AST DRP and annually conduct a live exercise that aligns with the DRP as required by State law.

Finding 2: Continuity of Operations Planning

Continuity of operations are intended to facilitate a timely and orderly resumption of critical business operations in the event of a disaster or other interruption of service. State law[6] requires the SDC to develop and implement a business continuity of operations plan (COOP) and, beginning July 1, 2015, and annually thereafter, conduct a live exercise of the COOP. State law[7] also requires that a disaster preparedness plan (i.e., COOP) include, at a minimum, the following elements: identification of essential functions, programs, and personnel; procedures to implement the plan and personnel notification and accountability; delegations of authority and lines of succession; identification of alternative facilities and related infrastructure, including those for communications; identification and protection of vital records and databases; and schedules and procedures for periodic tests, training, and exercises.

Our audit procedures disclosed that the AST COOP needs improvement. While periodic tests and exercises were referenced in the AST COOP, the specific frequency and type of periodic tests and exercises were not addressed except for quarterly Immediate Response Information System (IRIS) testing used to notify staff in the event of a disaster. According to AST records, a test of IRIS was performed on June 6, 2017, and the test results were provided to the process owner for evaluation and then used to update the contact lists and correct any contact information discrepancies. We reviewed the IRIS contact list as of September 20, 2017, to determine whether the 22 AST employees hired during the period January 1, 2017, through June 7, 2017, were on the contact list. While AST management stated the IRIS contact list is reviewed quarterly, we found that 8 employees (hired from January 19, 2017, through April 21, 2017) were not on the contact list. Additionally, the COOP did not include vital databases essential to reconstruct and continue the operations of the AST.

Absent a defined schedule for the conduct of tests and exercises of the COOP, an up-to-date contact list, and the identification of vital databases, the continuity of essential State functions and the availability of related information may be impaired. A similar issue was noted in our report No. 2017-087.

Recommendation: To ensure the continued operations of the SDC, we again recommend that AST management include all essential information in the COOP and periodically update the COOP to ensure that contact information is accurate and complete.

[6] Section 282.201(2)(c), Florida Statutes.

[7] Section 252.365(3)(b), Florida Statutes.

Finding 3: Inventory of IT Resources

Effective IT inventory controls include the maintenance of a complete, accurate, and up-to-date inventory of IT systems (e.g., physical and virtual servers) to ensure that management is knowledgeable of all IT systems for which they are responsible and that the IT systems are secured and configured as intended by management. Further, a complete, accurate, and up-to-date inventory is necessary for effective monitoring, testing, and evaluation of IT resources to ensure the timely implementation of the latest relevant security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors. AST rules[8] require that each State agency ensure that physical devices, systems, software platforms, and applications within the organization are inventoried and managed.

In Finding 4 of our report No. 2017-087 issued January 5, 2017, we noted that the inventory of IT resources at the SDC was not complete and, in some cases, was not accurate, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated to ensure the timely implementation of the latest security patches and other critical updates from IT vendors. In connection with that audit, we found that the AST maintained an inventory of the SDC-managed IT resources in a change management database (CMDB). Inventory items were recorded as configuration items (CIs) in the CMDB. The CIs included applications, databases, documents, network devices, storage items, applications, servers, and other IT infrastructure items. The CI information included such things as the operating system version, installed patches, system up-time, and maintenance notes. However, we found that some inventory items were not recorded as CIs and some CI information was inaccurate or incomplete.

Pursuant to State law,[9] the AST Inspector General provided a 6-month response dated July 5, 2017, on the status of corrective actions related to the findings in our report No. 2017-087. For Finding 4, the Inspector General's response stated that corrective action was complete as the CI types included in the CMDB were defined and included in the Configuration Management System Architecture (CMSA) document. However, in his August 2, 2017, response to our audit inquiry related to the CMSA document and the CMDB, the Deputy Director of Information Systems stated that the CMSA document was inaccurate and that the CMDB was not the repository of the SDC-managed inventory. He also stated that the repository of the SDC-managed inventory was not documented and that inquiries of management within each SDC section (Database Section, Open Systems Section, etc.) would be necessary to determine how each section tracked their managed devices.

We interviewed management in each SDC section and evaluated the completeness and accuracy of the inventory repositories identified by section management. We found that the various identified inventory repositories were not always complete and accurate. Specifically, the repositories for Windows servers, open systems servers, SQL servers, network devices, and primary storage hardware devices were incomplete or inaccurate.

[8] AST Rule 74-2.002(1)(a) and (b), Florida Administrative Code.

[9] Section 20.055(6)(h), Florida Statutes, requires the Inspector General to monitor the implementation of the agency's response to any report on the State agency issued by the Auditor General. No later than 6 months after the report publishes, the Inspector General must provide a written response on the status of corrective actions taken to the agency head and file a copy of the response with the Legislative Auditing Committee.

Maintenance of a complete, accurate, and up-to-date inventory of all IT resources is necessary to properly account for IT resources and facilitates the monitoring, testing, and evaluation of IT resources to ensure the timely implementation of the latest relevant security patches and other critical updates from IT vendors. Also, the inaccurate reporting of the status of corrective actions taken in response to audit findings may inhibit management's ability to effectively monitor the AST's efforts and progress in implementing appropriate corrective actions.

Recommendation: We recommend that AST management define and document the repository for each inventory item and update the CMSA document to include all identified repositories. Additionally, we recommend that AST management continue working to establish a complete, accurate, and up-to-date inventory of all SDC-managed IT resources. Management should also take appropriate actions to effectively monitor the efforts and progress made in implementing appropriate corrective actions for audit findings.

Finding 4: Backup Tape Reconciliations and Destruction

Effective backup controls include policies, procedures, and processes to ensure that accurate records of the location and status of backup data are maintained and all tapes are accounted for, allowing an entity to minimize the risk of data loss that may occur as a result of unexpected events. Such actions maintain the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

Our audit procedures disclosed that reconciliation policies and procedures were not in place during the 2016-17 fiscal year. While the AST initiated draft tape reconciliation procedures[10] on June 30, 2017, the procedures were not finalized until September 5, 2017. Our review of the finalized tape reconciliation procedures disclosed that the procedures were not comprehensive and lacked periodic review and reconciliation procedures between the backup systems that created the backup tapes and the tracking system used to move the tapes between the AST and the vendor used for offsite tape storage. In response to our audit inquiry, AST management in the Bureau of Infrastructure and Operations Support (Bureau of Infrastructure) responsible for the tracking of tapes and staff in Bureau of Core Services, Backup and Recovery Section (Backup Section) responsible for the managing and creating backup tapes, stated that, when the offsite storage vendor changed in June 2016, procedures were performed to reconcile all tapes moved from the prior offsite storage vendor to the current offsite vendor; however, no documentation of the reconciliation was maintained. Backup Section staff also stated that, while no documentation was maintained, a reconciliation between the tape backup systems and the tracking system had been performed for all currently used backup servers and that AST staff was working, as of January 16, 2018, to complete reconciliations for the backup servers that are not currently used but contain backup tapes that may be necessary for restoration.

Additionally, we requested reports of tapes written for all the backup servers for the primary backup system utilized by the SDC to determine whether the tapes listed in the backup server reports were also listed in the tracking system and the location of the tapes matched between the two systems. AST Backup Section staff were unable to provide us all the primary backup system reports; however, we compared the 6,904 tapes listed on the 4 reports provided (created July 26, 2017, August 14, 2017, August 16, 2017, and August 24, 2017) to the tracking system and found that the offsite location status

[10] Reconciliation of Tapes, AST-BIF-P-214.

listed in the backup server reports for 1,138 tapes did not match the tapes' location recorded in the tracking system. Additionally, 4 tapes listed with offsite location status in the backup server reports were not recorded in the tracking system. In response to our audit inquiry, Backup Section management stated on November 16, 2017, that the AST was still performing a complete tape reconciliation between the backup systems and the tracking system, and that the reconciliation was a manual process that would continue for some time due to manpower limitations.

We also reviewed 41 of the 2,818 backup tape records that were marked in the tracking system as destroyed during the period June 1, 2016, through August 22, 2017, to evaluate whether the appropriate approvals were obtained and records of destruction were maintained. Our audit procedures, including inquiries of AST staff, disclosed that 20 of the 41 tapes had not been physically destroyed. In response to our audit inquiry, Bureau of Infrastructure management stated that AST staff erroneously marked tapes as destroyed whenever there were scanning errors associated with the tapes. Subsequent to our audit inquiry, Bureau of Infrastructure staff requested information from the tracking system vendor on September 22, 2017, regarding how to delete future scanning errors so that only physically destroyed tapes are marked as destroyed in the tracking system. Our evaluation of the records for the remaining 21 tapes marked as destroyed disclosed that records of approval and destruction were not always available. Specifically, AST records did not evidence approvals for 15 of the 21 tapes destroyed. Additionally, the destruction records for 5 of the 21 tapes destroyed were not accurate as the records were date stamped as destroyed in January 2017 and Bureau of Infrastructure management stated that the tapes were not destroyed until sometime in July 2017.

The lack of policies and procedures providing guidance on backup tape reconciliations and inaccuracies in tape records may limit the SDC's ability to locate backup tapes and timely and completely recover information in the event of a loss of production data. Additionally, without documented approvals prior to tape destruction, tapes that are necessary to restore customer data files may be destroyed. A similar finding was noted in our report No. 2017-087.

Recommendation: We again recommend that AST management improve backup controls to include comprehensive policies and procedures to help ensure the accuracy of AST backup tape location records and the timely reconciliation of the backup systems that create backup tapes and the tracking system used to move tapes to the offsite storage vendor. We also recommend that AST management ensure that documented approval for destruction be obtained before a backup tape is destroyed, backup tapes approved for destruction are timely destroyed, and accurate records of destruction are maintained.

Finding 5: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. State law[11] requires the AST to assume administrative access rights (privileges) to resources and equipment, including servers, network components, and other devices, consolidated into the SDC. Additionally, State law[12] requires State agencies to relinquish administrative rights to

[11] Section 282.201(2)(f), Florida Statutes.

[12] Section 282.201(2)(f)1., Florida Statutes.

consolidated resources and equipment. The SDC is allowed by State law[13] to provide customer entities with access to applications, servers, network components, and other devices necessary for entities to perform business activities and functions. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Our audit procedures disclosed the existence of user accounts with administrative access privileges to consolidated resources and equipment that were not assigned to AST staff. In response to our audit inquiry, AST management stated that the accounts were assigned to customers for administration of the customers' resources. However, the AST was unable to demonstrate at the time of our testing that the AST had verified with the respective customers that the accounts continued to be necessary and appropriate. Specifically, we noted that:

- For the Access Control Facility 2 (ACF2) mainframe security environment applicable to one State agency's logical partition (LPAR),[14] 16 of the 37 active accounts with one or more administrative access privileges that included the ability to establish user accounts and create or modify access rules to programs and files were assigned to the State agency's staff as of August 14, 2017.
- For the Resource Access Control Facility (RACF) mainframe security environment applicable to four LPARs, 27 of the 48 active accounts with one or more of the administrative access privileges that included the ability to copy, reorganize, catalog, and scratch user or data sets, specify logging options, and have full control over all RACF user profiles as of August 14, 2017, were assigned to staff at State agencies.
- For the CA Top Secret mainframe security environment applicable to one State agency's LPAR, 5 of the 17 active accounts with one or more administrative access privileges as of August 21, 2017, were assigned to the State agency's staff.
- For 40 of 2,195 Windows production servers, as of September 7, 2017, privileges to 21 of the 111 local *Administrator* accounts were assigned to staff at State agencies.

Additionally, our audit procedures disclosed the existence of user accounts assigned to AST SDC staff with domain[15] administrator access privileges to two of the nine AST network domains that were not appropriate. Specifically, as shown in Table 1, 17 of the 77 active accounts with domain administrator access privileges assigned to SDC staff were not appropriate based on the job duties assigned to the respective SDC staff.

Table 1
Inappropriate Domain Administrator Access Privileges

	Number of Active Accounts with Domain Administrator Access Privileges		
Network Domain	Assigned to SDC Staff	Inappropriately Assigned to SDC Staff	Date of Audit Review
1	46	16	July 31, 2017
2	31	1	July 31, 2017
Total	**77**	**17**	

[13] Section 282.201(2)(f)2., Florida Statutes.

[14] A logical partition, commonly called an LPAR, is a subset of a computer's hardware resources, virtualized as a separate computer. In effect, a physical machine can be partitioned into multiple logical partitions, each hosting a separate organizational environment if desired.

[15] A domain is a form of computer network in which all user accounts, computers, printers, and other security principles, are registered with a central database located on one or more clusters of central computers known as domain controllers.

In response to our audit inquiries, AST management indicated that, as of November 8, 2017, 2 of the 17 accounts had been disabled.

We also noted that certain IT security controls related to access need improvement. To avoid the possibility of compromising SDC customer entity data and related IT resources, we are not disclosing in this report the specific details of what we found. However, we have notified appropriate AST management of the specific issues.

Inappropriate or unnecessary access privileges to mainframe, open systems, and Windows server environments and the interconnected network domains and devices increase the risk of unauthorized modification, loss, or disclosure of data and IT resources. A similar finding was noted in our report No. 2017-087.

Recommendation: To promote compliance with State law and an appropriate separation of duties, we again recommend that AST management appropriately restrict user access privileges to mainframe and Windows server environments and the interconnected network domains to only those functions necessary for the user's assigned job duties.

Finding 6: Periodic Review of Access Privileges

Effective access controls include policies and procedures for the periodic review of user access privileges based on risk, access account change activity, and error rate. Such reviews help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Although the AST had not developed a comprehensive policy for the periodic review of access privileges, two bureaus had established procedures for such reviews. Specifically:

- The Bureau of Central Services established an *Interim Account Access Monitoring Procedure* on July 20, 2017, that required the review of accounts assigned to current and former staff within the various sections of the Bureau. However, our review of the procedure disclosed that a comprehensive review from a system-generated access list was not required. Without a comprehensive review from a system-generated access list, accounts assigned to staff outside the Bureau may not be subject to review.
- The Bureau of Windows Services established the *AST-BWS-AP-0001, Active Directory Account Audit Procedure* on June 22, 2017. While the procedure specified that two reports listing domain administrator access would be generated biweekly and sent to the Windows Services Bureau Chief (or designee) and the ISM (or designee) for review, the procedure did not require a response from the reviewers. In response to our audit inquiry, AST management stated that reviewers would initiate an access change request if changes were necessary, but otherwise documentation of the reviews was not maintained.

The Network Section within the Bureau of Core Services performed a process similar to that performed by the Bureau of Windows Services; however, the procedure was not documented.

Our audit procedures also disclosed that AST staff had not conducted a periodic review of all Oracle database administration accounts to establish whether the AST or the customer whose data resides on the database was responsible for the administration accounts. Specifically, for the six Oracle database clusters reviewed, AST management stated that AST staff only utilized 2 accounts on each database

cluster to administer the Oracle databases; however, AST records did not demonstrate that the remaining database administration accounts were assigned to the applicable State agency customers.

Without a documented process for performing a comprehensive access privileges review utilizing system generated lists, management's assurance that user access privileges were authorized and appropriate is limited. A similar finding was noted in our report No. 2017-087.

Recommendation: We recommend that AST management develop and implement a comprehensive policy for the periodic review of access privileges and maintain documentation of the reviews conducted.

Finding 7: Backup Controls

State law[16] requires the SDC to ensure proper data backup and data recovery. The SDC's service-level agreements (SLAs) with customer entities require the SDC, at a minimum, to perform incremental data backups daily and full data backups weekly.

Our review of backup procedures performed for 42 of the 2,195 production physical and virtual Windows servers and 20 of the 197 Red Hat Enterprise Linux nontest, nondevelopment open systems servers disclosed that AST backup controls need improvement. We found that the AST had not timely backed up 6 of the 62 selected servers, specifically:

- The AST had not timely backed up 2 of the 42 Windows servers as of September 1, 2017. The AST was unable to demonstrate that 1 of the 2 servers had ever been backed up or that the server was included in the automated backup process. Although the other server was included in the automated backup process, the server had not been backed up since July 6, 2017.
- The AST had not timely backed up 4 of the 20 open systems servers as of September 7, 2017. The AST was unable to demonstrate that 2 of the 4 open systems servers had ever been backed up or that the servers were included in the automated backup process. Although the other 2 servers were included in the automated backup process, the servers had not been backed up since August 29, 2017, and September 2, 2017, respectively.

In response to our audit inquiry, AST management stated that back up was not required for the 3 servers (1 Windows server and 2 open systems servers) that were not backed up; however, AST records did not demonstrate that backups were not necessary.

Additionally, on October 20, 2017, we observed that a backup job within an AST backup system had been running continuously for 71 hours, thereby preventing other backup jobs from running. Upon audit inquiry, AST Backup Section staff stated that the backup job was for a daily backup that normally took 2 hours to complete. The Chief of Production System Services indicated that the staff person responsible for monitoring backups had been out sick for 3 days and no one had noticed the backup was still running and preventing other backups jobs.

Timely server backups ensure that customer data is readily recoverable when needed in response to an unexpected event. A similar finding was noted in our report No. 2017-087.

[16] Section 282.201(2)(b), Florida Statutes.

Recommendation: We again recommend that AST management ensure that all required server backups are timely and successfully performed and, for any servers not requiring backup, proper documentation is maintained to demonstrate that backups are not necessary.

Finding 8: Software Licensing

AST rules[17] require each agency to establish policies and procedures to manage and monitor the agency's regulatory, legal, risk, environmental, and operational IT requirements. Documented policies and procedures related to the management and monitoring of software licensing agreements that include prohibiting violations of software licensing agreements and restricting the use of personal and public domain software help ensure compliance with software licensing agreements.

The AST lacked comprehensive policies and procedures related to the management and monitoring of software licensing. In a January 24, 2018, response to our audit inquiry, AST management stated that they were in the process of drafting a *Software Asset Management Policy* and that a software asset management tool had been purchased and was expected to be implemented by March 2018 to help ensure compliance with software licensing agreements.

The absence of comprehensive policies and procedures for managing and monitoring software license agreements increases the risk of violations of such agreements.

Recommendation: We recommend that AST management complete the establishment of comprehensive policies and procedures related to the management and monitoring of software licensing agreements.

Finding 9: Performance Metrics

Effective IT performance management requires a monitoring process that includes defining relevant performance metrics and the systematic and timely reporting of performance in relation to the performance metrics. Pursuant to State law,[18] the SDC is to establish in the SLAs with customer entities the metrics and processes by which the business standards for each service provided to the customer entities are to be objectively measured and reported.

The SLAs required Oracle database uptime to be a minimum of 99.5 percent of the scheduled availability for the respective database. As part of our audit procedures, we reviewed the performance metrics reported in the monitoring tool that measures Oracle database uptime for 7 database clusters and 25 database instances for 11 selected State agency customers for the month of April 2017. According to the performance metrics reported, the SDC did not meet its performance target for 2 of the selected State agency customers (1 database instance for the Department of Environmental Protection and 1 database instance for the Department of Transportation), as the Oracle database uptime was less than 99.5 percent of the scheduled availability. Additionally, for 9 database instances for 6 State agency customers, there were no performance metrics available in the monitoring tool. In response to our audit

[17] AST Rule 74-2.002(3), Florida Administrative Code.

[18] Section 282.201(2)(d)5., Florida Statutes.

inquiry, AST management stated that, due to software migration to an upgraded version of the monitoring tool, the metrics prior to migration no longer existed.

To evaluate the accuracy of the uptime statistic reported, we reviewed the monthly performance metric reports for 4 selected database instances that listed Oracle database performance statistics, including blackout periods (database downtime due to maintenance), to evaluate whether the downtimes were scheduled and, therefore, should not be subtracted from the uptime performance metric for the month. While the AST provided service tickets for 2 of the 4 database instances, the tickets did not contain sufficient detail to support that the blackout period was for scheduled maintenance. For the other 2 database instances, AST records did not evidence that the blackout period was for maintenance.

Effective database performance monitoring is essential to the timely detection and resolution, as applicable, of critical incidents involving database services. Additionally, without complete records the AST cannot demonstrate the accuracy of reported uptime statistics or compliance with the SLA performance metrics. A similar finding was noted in our report No. 2017-087.

Recommendation: We again recommend that AST management ensure that SDC database performance uptime metrics included in the SLA agreements are met and that appropriate documentation for uptime performance statistics is maintained.

Finding 10: Computer Security Incident Response Team

AST rules[19] require agencies to establish a Computer Security Incident Response Team (CSIRT) to respond to detected cybersecurity events. Among other things, the responsibilities of the CSIRT members include: convening at least quarterly to review, at a minimum, established processes and escalation protocols; receiving training at least annually on cybersecurity threats, trends, and evolving practices, and training that is coordinated as a part of the information security program.

Our audit procedures disclosed that the AST CSIRT did not convene at least quarterly during the 2016-17 fiscal year as the AST did not establish the CSIRT until February 7, 2017, and the CSIRT's initial meeting was not held until June 16, 2017. Additionally, annual CSIRT member training on cybersecurity threats, trends, and evolving practices was not provided for the 2016-17 fiscal year. In response to our audit inquiry, AST management stated that the CSIRT members completed the required training in February 2018.

Quarterly CSIRT meetings, to review established processes and escalation protocols, and annual CSIRT member training promote prompt and appropriate responses to cybersecurity events.

Recommendation: We recommend that AST management ensure that CSIRT meetings are conducted at least quarterly and that CSIRT members receive annual training as required by AST rules.

[19] AST Rule 74-2.005(1)(a), Florida Administrative Code.

Finding 11: Security Controls – Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, Shared Accounts, Service Accounts, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related tape encryption, vulnerability management, configuration management, user authentication, shared accounts, service accounts, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising SDC customer entity data and related IT resources. However, we have notified appropriate AST management of the specific issues.

Without appropriate security controls related to tape encryption, vulnerability management, configuration management, user authentication, shared accounts, service accounts, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of customer entity data and related IT resources may be compromised. Similar findings related to vulnerability management, configuration management, user authentication, service accounts, and logging and monitoring were communicated to AST management in connection with our report No. 2017-087.

Recommendation: We recommend that AST management improve certain security controls related to tape encryption, vulnerability management, configuration management, user authentication, shared accounts, service accounts, and logging and monitoring to ensure the confidentiality, integrity, and availability of SDC customer entity data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the AST had taken corrective actions for the applicable findings included in our report No. 2017-087.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from July 2017 through December 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected AST IT controls applicable to State Data Center (SDC) Operations during the period July 2016 through December 2017 and selected actions subsequent thereto. The overall objectives of the audit were:

- To evaluate the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other

guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources at the SDC.

- To determine whether management has corrected, or is in the process of correcting, deficiencies disclosed in audit report No. 2017-087 that are applicable to the scope of this audit.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the SDC controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the SDC controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the SDC controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of SDC controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed AST personnel and obtained an understanding of the organizational structure, statutory requirements, key policies, procedures, and operational processes for the AST and the SDC.
- Obtained an understanding of the IT infrastructure and architecture of the SDC, including hardware, software, and operating systems for the various server platforms and network components, and database management systems.
- Evaluated the AST's compliance with contractual requirements for performance uptime monitoring. Specifically, we reviewed:
    - The monthly performance metrics for 7 of the 32 production Oracle database clusters and 25 of the 222 production Oracle database instances for the month of April 2017 to evaluate whether AST met its monthly uptime performance metric.

- The monthly performance metric reports for 4 Oracle database instances to evaluate the accuracy of the uptime performance statistics reported, including documentation for scheduled downtimes.
- The monthly uptime performance reporting system for the mainframe environment.

- Evaluated the effectiveness of AST procedures for vulnerability management including analysis and remediation of reported vulnerabilities for the SDC's network, mainframe, Windows, and open systems environments.
- Evaluated the adequacy of the SDC's IT resource inventory recording procedures. Specifically, we compared:
  - 40 of the 2,905 active Windows servers listed in the CMDB as of September 6, 2017, to the Windows server inventory repository.
  - 40 of the 896 active open systems servers listed in the patch management system to the open systems server inventory repository as of September 18, 2017.
  - 40 of the 1,245 active SQL Server database instances listed in the CMDB to the SQL Server inventory repository as of September 6, 2017.
  - 40 of the 295 active Oracle database instances listed in the CMDB as of August 3, 2017, to the Oracle inventory repository.
  - The 107 network devices listed in a network management tool to the physical inventory tracking system as of August 8, 2017.
  - 35 primary storage hardware devices listed in their applicable management tool to the physical inventory tracking system as of August 8, 2017.
  - The 2 active DB2 database instances listed in the DB2 inventory repository as of September 5, 2017, to the CMDB.
- Evaluated the effectiveness of the SDC's software and IT infrastructure component change control process including hardware and system software changes, firewall changes, and patch management. Specifically, we reviewed:
  - 10 of the 44 closed, fulfilled, major change requests during the period July 1, 2016, through June 30, 2017, to determine whether hardware and systems software changes were appropriately authorized, tested, functioned as intended, and approved.
  - 5 of the 25 closed, fulfilled, emergency change requests during the period July 1, 2016, through June 30, 2017, to determine whether hardware and systems software changes were appropriately authorized, tested, functioned as intended, and approved.
  - 20 of the 197 Red Hat Enterprise Linux production open systems servers to evaluate whether, as of September 25, 2017, the SDC had timely installed vendor-supplied patches.
  - 12 selected network high-risk devices to evaluate whether, as of August 28, 2017, the SDC timely installed vendor-supplied patches.
  - 6 of the 32 Oracle database clusters to evaluate whether, as of September 29, 2017, the SDC timely installed vendor-supplied patches.
- Evaluated the effectiveness of the SDC logging and monitoring controls.
- Determined whether the AST had developed continuity of operations and disaster recovery plans and whether the SDC had conducted a live exercise of each plan as required by Section 282.201(2)(c), Florida Statutes.
- Evaluated the effectiveness of the SDC's backup processes, including tape and disk backup procedures, backup tape reconciliation processes, and tape destruction. Specifically, we:

- Examined backup reports for 42 of the 2,195 production physical and virtual Windows servers as of September 1, 2017, and 20 of the 197 nontest, nondevelopment Red Hat Enterprise Linux open systems servers as of September 7, 2017, to determine whether required backups were performed.
- Compared backup server tape records for 6,904 Windows servers and open systems backup tapes listed as being stored at an off-site storage facility to the tracking system records to determine the accuracy of the records.
- Examined tape destruction records for 41 of the 2,818 tape records with a destroyed status as of August 22, 2017, to determine whether required approvals were documented and accurate records of destruction were maintained.

- Evaluated the logical design, authorization, administration, and periodic review procedures for logical access privileges to SDC IT resources and customer entity data. Specifically, we reviewed:
  - The appropriateness of administrative access privileges for the 9 network domains used for SDC services and operations as of July 31, 2017, August 16, 2017, and August 21, 2017.
  - The appropriateness of access privileges for the 48 RACF administrative accounts with selected high-risk access privileges for 4 mainframe LPARs as of August 14, 2017.
  - The appropriateness of access privileges for the 48 ACF2 administrative accounts with selected high-risk access privileges for 1 mainframe LPAR as of August 14, 2017.
  - The appropriateness of access privileges for the 17 CA Top Secret administrative accounts with administrative access privileges for 1 mainframe LPAR as of August 21, 2017.
  - The appropriateness of access privileges for the 20 administrative accounts for 20 selected open systems servers as of September 25, 2017.
  - The appropriateness of access privileges for the 65 administrative accounts for 12 selected network devices as of August 24, 2017.
  - The appropriateness of access privileges for 111 selected accounts with administrative access privileges to their respective Windows server environments as of September 7, 2017.
  - The appropriateness of access privileges for 6 of 32 Oracle database clusters as of September 29, 2017.
- Evaluated the effectiveness of the SDC's IT infrastructure user authentication controls. Specifically, we reviewed:
  - RACF user authentication controls for 4 mainframe LPARs as of August 14, 2017.
  - ACF2 user authentication controls for 1 mainframe LPAR as of August 14, 2017, and August 21, 2017.
  - CA Top Secret user authentication controls for 1 mainframe LPAR as of August 21, 2017.
  - User authentication controls for 9 selected network domains as of July 31, 2017, August 16, 2017, and August 21, 2017.
  - User authentication controls for 20 selected open systems servers as of September 25, 2017.
  - User authentication controls for 12 selected high-risk network devices as of August 24, 2017, and December 5, 2017.
  - User authentication controls for 6 of 32 Oracle database clusters as of September 29, 2017.
- Evaluated the adequacy of the policies, procedures, and processes for SDC capacity planning and the management and monitoring of software licensing.

- Evaluated whether the AST's data loss prevention procedures were sufficient for the identification, usage, monitoring of confidential and sensitive information.
- Evaluated whether the AST's policies, procedures, and process for incident response were sufficient including the establishment of a CSRIT in compliance with AST rules to respond to cybersecurity threats.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA
Auditor General

EXHIBIT A

LIST OF STATE DATA CENTER CUSTOMER ENTITIES

AS OF DECEMBER 31, 2017

	Entity Name
1	Agency for Health Care Administration
2	Agency for Persons with Disabilities
3	Children's Home Society of Florida
4	Department of Business and Professional Regulation
5	Department of Children and Families
6	Department of Citrus
7	Department of Corrections
8	Department of Economic Opportunity
9	Department of Education
10	Department of Elder Affairs
11	Division of Emergency Management
12	Department of Environmental Protection
13	Department of Health
14	Department of Highway Safety and Motor Vehicles
15	Department of Juvenile Justice
16	Department of Lottery
17	Department of Management Services
18	Department of Military Affairs
19	Department of Revenue
20	Department of State
21	Department of Transportation
22	Department of Veterans' Affairs
23	Executive Office of the Governor
24	Florida Commission on Human Relations
25	Florida Fish and Wildlife Conservation Commission
26	Greater Orlando Aviation Authority
27	Justice Administrative Commission
28	Miami-Dade Expressway Authority
29	Northwest Florida Water Management District
30	Public Employee Relations Commission
31	Public Service Commission
32	Santa Rosa County

Source: AST Records.

MANAGEMENT'S RESPONSE

State of Florida
Agency for State Technology

4050 Esplanade Way, Suite 115
Tallahassee, FL 32399-0950
Tel: 850-412-6050

Rick Scott, Governor

Eric M. Larson
State CIO/Executive Director

Response to Preliminary and Tentative Audit Findings

March 12, 2018

Sherrill F. Norman, CPA
Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to section 11.45(4)(d), Florida Statutes, attached is the Agency for State Technology's (AST) response to the Preliminary and Tentative Audit Findings and Recommendations on State Data Center Operations.

We have attempted to provide thoughtful, written responses to findings showing that we are receptive to constructive review, continue to engage appropriate corrective action, and continue to be a good steward of the public's resources and trust.

Because of the close timing of the audits, AST unfortunately has insufficient time to fully engage and complete respective corrective action, resulting in repeat audit findings as illustrated in this report. Specifically, nine of the eleven audit findings in the report were noted as similar issues from the prior report. We respectfully ask that the Auditor General's (AG) office revisit this timing so AST has sufficient time between audits to make progress on corrective action and also to enhance the outcome of future audits as audit staff will be able to focus on new areas during their evaluation.

Additionally, to improve the efficiency of the audit process for both AG and AST staff, we respectfully request the AG consider taking a platform-based instead of a general controls approach to future audits. This will allow for focused evaluation of controls, allow AG staff to work with specific AST staff, get a complete view of platform processes, and increase the process efficiency by reducing the likelihood of overlapping inquiries, etc.

If you have any questions concerning AST's response, please contact Tabitha McNulty, Inspector General, at (850) 412-6022.

Sincerely,



Eric M. Larson, State CIO/Executive Director
Agency for State Technology

attachment

cc: Robert Thompson, Chief Operations Officer
Tabitha McNulty, Inspector General

Agency for State Technology
Corrective Action Plan

Information Technology Operational Audit of the Agency for State Technology, State Data Center Operations

Finding # 1

Finding Title: Disaster Recovery Planning

Platform: Core Services – Disaster Recovery

Finding Statement:

The State Data Center's [SDC] disaster recovery plan [DRP] and annual testing continue to need improvement to ensure that critical State Data Center operations are recovered and continue in the event of a disaster or other interruption in service.

Recommendation:

To ensure recoverability of the critical SDC applications in the event of a disaster or other interruption of service, we recommend that AST management continue development and implementation of a comprehensive AST DRP and annually conduct a live exercise that aligns with the DRP as required by State law.

Program Response:

The Agency for State Technology (AST) has recently authored the AST DRP and has conducted an annual live exercise.

AST conducted the first live exercise of its DRP on June 19, 2017, and has scheduled recurring annual tests. This ongoing testing will further evidence that critical State Data Center applications can and will be timely and orderly restored.

The technologies employed by AST automate the failover and fail back of critical resources and minimize the need for detailed instructions during a disaster. The AST DRP specifies the configuration of the virtual environment, how it uses Site Recovery Manager (an industry standard disaster recovery (DR) product), and the steps required to facilitate service recovery during a recovery event.

For items that require manual failover, the DR tools include guidance when the process is initiated, rendering separate hardcopy documentation both redundant and a source of unnecessary maintenance overhead for the agency. Since the DRP is based on the procedures for staff's daily work activities, links will be added to direct employees to current policies and procedures for additional information as necessary.

The live annual test of AST selected critical systems was completed in under an hour, as noted within the audit report. Conducting a DR test successfully within that time period for the tested applications demonstrates the sophistication and capability of the DR service offering available for critical business

systems. Even though AST decided not to test everything listed in the plan, AST will ensure the DRP aligns with the testing activities in subsequent tests.

For the remainder of systems that are not protected by the automated processes, DR restoration activities are no different than the routine restoration requests made by customers and handled on a day-to-day basis. File, database, and system restores leverage the same procedures used day-in and day-out by the teams to conduct normal operations. Similar to the automated processes described earlier, AST will add links to the DRP directing employees to current policies and procedures for additional information as necessary. The value and benefit of the AST DR solution design is that, for the first time in Florida's history, all SDC customers' data are programmatically replicated to the DR site. Restores of data and systems are now possible in minutes or hours, instead of days or weeks and that restoration process is now routinely operationalized. Operating as designed, services and systems can be restored using standard tools and procedures any qualified system administrator would be capable of performing.

Due to the rapidly changing nature of operational environments, continuous improvements of the DRP are expected and incorporated in AST's approach to test planning, test execution, and plan updates. The annual lifecycle of the DRP is to conduct tests to improve planning, execution, and updates to the DRP. As DRP tests are conducted and any gaps in specific recovery processes or documentation identified, the DRP will be updated as necessary to continually improve the process.

Finding # 2

Finding Title: Continuity of Operations Planning

Platform: Core Services – Disaster Recovery

Finding Statement:

> The State Data Center's continuity of operations plan [COOP] and testing continue to need improvement to ensure the timely resumption of critical business operations in the event of a disaster or other interruption in service.

Recommendation:

> To ensure the continued operations of the SDC, we again recommend that AST management include all essential information in the COOP and periodically update the COOP to ensure that contact information is accurate and complete.

Program Response:

Business processes evolve constantly which results in corresponding changes to the supporting environments. As a result, COOP require ongoing maintenance. COOP documentation updates most often occur after the execution of COOP tests, as this is the time when most opportunities for improvement are identified. As part of the continuous improvement process, AST had already identified and resolved two items cited in this finding and continues to conduct successful operational tests allowing for identification of any areas that require further refinement.

As part of these improvements, on December 12, 2017, AST implemented an online Employee Action Module within AST's IT Service Management (ITSM) system to replace a manual form-based process. This new ITSM workflow was implemented to manage the actions associated with employee new hires, separations, and internal transfers. A component of this workflow is to ensure the update of contact information in the Immediate Response Information System (IRIS). This process change will help to ensure that staff contact information is accurate and complete.

Additionally, to help ensure 100% enrollment in the IRIS system, periodic IRIS testing is conducted which includes staff notifications requesting verifying receipt of corresponding messages and steps to take if staff do not receive IRIS alerts. Although the recently implemented process improvements will ensure tasks are tracked to completion, the manual steps required to update the IRIS system compete with other manual tasks before being implemented. Due to the delays introduced by these manual processes, AST is evaluating replacement solutions to automate this synchronization and ensure perpetual reconciliation.

The audit report indicated that vital databases are not specifically listed in the AST COOP. The databases deemed critical for operations are listed in the AST DRP. To further satisfy the recommended improvements, AST added informational links to the AST DRP into the AST COOP documents that include vital database information.

Finding # 3

Finding Title: Inventory of IT Resources

Platform: Windows, Central Services, Core Services, ITSM, and Operations

Finding Statement:

AST management had not defined the repositories for the inventory of IT resources at the State Data Center and the inventories maintained were not complete and, in some cases were not accurate, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated to ensure the timely implementation of the latest security patches and other critical updates from IT vendors.

Recommendation:

We recommend that AST management define and document the repository for each inventory item and update the CMSA document to include all identified repositories. Additionally, we recommend that AST management continue working to establish a complete, accurate, and up-to-date inventory of all SDC-managed IT resources. Management should also take appropriate actions to effectively monitor the efforts and progress made in implementing appropriate corrective actions for audit findings.

Program Response:

AST has numerous, often overlapping management tools within various contexts for what could be considered "IT systems" or "IT resources."

Examples of tools that contain an inventory of IT resources include: AST's endpoint management tool, enterprise monitoring system, virtualization management, backup system, data center infrastructure management, converged compute infrastructure monitoring, security and threat detection and response systems, badging systems, camera systems, phone/voice systems, air conditioning systems, Uninterrupted Power Supply (UPS) and generator systems, under-floor water sensors, heat sensors and many others.

Many IT resources that exist in one repository cannot exist in another due to the different contexts of each system. For example, a single physical IT asset represents over 100 different physical IT resources monitored by the hardware monitoring tool and over 3,000 virtual IT resources that are actively monitored within the virtualization management tool. The reconciliation of the inventory of physical, virtual, and logical resources may result in data inconsistencies.

To address the finding, AST is working to document the context of the various tools used to manage the various IT resources and continues to work with customer agencies to ensure that complete resource metadata is entered into the Configuration Management Database (CMDB).

Additionally, in August, AST hired a full-time dedicated Compliance Manager, for the explicit purpose of keeping track of all the internal, external, local, state, and federal audit and compliance requirements of the SDC. This resource also is responsible for tracking corrective actions of audit findings until they are resolved.

Finding # 4

Finding Title: Backup Tape Reconciliations and Destruction

Platform: Core Services – Backup and Recovery, Infrastructure and Operations – Tape Management

Finding Statement:

AST policies, procedures, and processes for reconciling and tracking backup tapes need improvement to ensure all backup tapes are accounted for and location and status records are accurate.

Recommendation:

We again recommend that AST management improve backup controls to include comprehensive policies and procedures to help ensure the accuracy of AST backup tape location records and the timely reconciliation of the backup systems that create backup tapes and the tracking system used to move tapes to the offsite storage vendor. We also recommend that AST management ensure that documented approval for destruction be obtained before a backup tape is destroyed, backup tapes approved for destruction are timely destroyed, and accurate records of destruction are maintained.

Program Response:

The AST Tape Management group follows the Magnetic Media Destruction procedure that is currently in place. AST did not find tapes that should have been retained were inappropriately destroyed; however, AST acknowledges that authorization for tape destruction should be retained, and in specific instances

the retention of records supporting the authorization of destruction could be improved. The processes and the supporting procedures have undergone constant migrations and revisions through initial customer agency data center consolidation, then SDC consolidation, off-site storage migration, and the disaster recovery operations center integration. Additionally, the agency reduced the number/versions of tape management solutions from over 56 to the few remaining systems. Because of the various projects and process changes, the procedure is currently undergoing another revision. Since this is a cross platform procedure, both the Backup team and Tape Management team participate in continuous monitoring and implement improvements as the processes and tools evolve and mature.

It is important to note that in addition to constantly attempting to stabilize the process, the teams undertake continuous improvements including the Tape Management team performing monthly reconciliation of all tapes located in the AST vault and the tape tracking tool, and the tracking and reconciling of tapes between the offsite vendor and AST. Further, the Backup team continues remediation of all library backup software to reconcile the multiple databases with the tape tracking tool.

While the audit report noted 1,138 tape record discrepancies, AST has determined that the tracking system contained the accurate tape location; however, the various backup systems were not always updated with this information, which is a time-consuming manual process to keep updated. While AST has unsuccessfully attempted to reconcile these repositories in the past, as noted within the audit, AST has since redefined the scope of this process to solely reconcile the inventory of the tapes among the various backup systems and the tape tracking system excluding specific location information to avoid confusion in the future.

Finding # 5

Finding Title: Appropriateness of Access Privileges

Platform: Central Services – Mainframe, Open Systems, Windows Bureau – Windows Platform

Finding Statement:

Some access privileges did not promote an appropriate separation of duties or were not appropriate based on the user's assigned job duties.

Recommendation:

To promote compliance with State law and an appropriate separation of duties, we again recommend that AST management appropriately restrict user access privileges to mainframe and Windows server environments and the interconnected network domains to only those functions necessary for the user's assigned job duties.

Program Response:

It should be noted that reviewing 28 audit reports covering 14 agencies in the past three years found findings related to appropriateness of access privileges repeated 26 times. The pervasiveness of these findings illustrates that the issues are large, dynamic, and complex and do not lend to simple procedural resolutions.

AST statutorily holds the authority to provide access to any system for the purposes of granting agency access to any "business function". In many cases, such as with user provisioning, the business function requires some administrative privilege due to the lack of technical options to granularly delegate more specific privileges. AST is continuing to implement a privileged identity and access management system that will provide additional granularity for business function delegation. Absent granular delegation, AST maintains that the concept of agencies relinquishing administrative rights does not preclude AST from delegating selective administrative rights should the business function require it. AST will continue to work with customers to evaluate and verify that administrative accounts are appropriate and retain documentation evidencing approvals for the accounts.

For the Mainframe platform, the attribute to allow full control over all Resource Access Control Facility (RACF) user profiles has been removed from all agencies as of January 31, 2018.

The finding also states that inappropriate domain administrator level rights were assigned to SDC staff. It is AST's responsibility to determine appropriate access for specific employee job functions. It is in the state's best interest to provide the necessary access to appropriately skilled technicians independent of organizational chart position to increase uptime, reduce cost, and provide the best possible customer service. To address this issue moving forward, AST will improve the associated documentation that identifies the need for these specific privileges within related job duties.

Finding # 6

Finding Title: Periodic Review of Access Privileges

Platform: Windows; Central Services; Core Services

Finding Statement:

The AST lacked a policy for comprehensive periodic access reviews and the various AST Bureau procedures for the performance and documentation of access reviews need improvement to ensure assigned access remains appropriate.

Recommendation:

We recommend that AST management develop and implement a comprehensive policy for the periodic review of access privileges and maintain documentation of the reviews conducted.

Program Response:

As stated in the finding, AST has several procedures for the review of access privileges; however, AST has not established an overall agency policy for periodic access review that outlines the expectations of management. While processes to conduct periodic access reviews were established in response to a similar audit finding from the previous year, this finding cites the absence of documentation for the review processes as an opportunity for improvement.

Although increasing the documentation level of effort for everyone involved will create additional auditable artifacts, the AST will attempt to automate the audit trail to provide for documented management review while minimizing additional workload for staff.

Finding # 7

Finding Title: Backup Controls

Platform: Core Services – Backup and Recovery

Finding Statement:

State Data Center backup controls continue to need improvement to ensure backups for all IT resources requiring backup are appropriately performed and customer data is readily recoverable in response to an unexpected event.

Recommendation:

We again recommend that AST management ensure that all required server backups are timely and successfully performed and, for any servers not requiring backup, proper documentation is maintained to demonstrate that backups are not necessary.

Program Response:

AST maintains that management has implemented appropriate process controls to ensure backups are appropriately performed. While product failures resulted in backup failures, the Backup and Recovery Section works 24x7x365 to meet Service Level Agreement (SLA) targets for the Data Protection Service and provides continuous improvement (as evidenced by improved backup metric compliance). The AST primary backup environment currently services approximately 3,600 clients, and generates 13,000 – 14,000 backup jobs per day, all of which require continuous monitoring.

Although AST's current primary backup software is provided by a well-known industry leader, major components of the primary backup product have suffered from vendor-acknowledged bugs and product failures which have required extensive manpower support. Since the completion of the audit (and due to the ongoing product failures), AST has initiated an effort to replace the problematic components. At the time of this writing, a replacement backup product has been procured and is being implemented. The replacement solution will also provide an expansion of recovery capabilities, facilitate expansion of enterprise data protection infrastructure to the cloud, and provide additional automation to discover any unprotected resources within the environment.

To further ensure the completion of backup jobs, AST implemented a backup audit process as a quality assurance measure. These backup audits are now memorialized SLA commitments, and presented to each customer for their review, update, and written concurrence. To date, AST has completed thirteen customer backup audits and repeated two customer audits due to failures of the backup product. There are 24 customer backup audits scheduled to be completed over the next calendar year.

AST also implemented an exception request form in August 2016 that included exceptions for the Data Protection Service. The Backup and Recovery team reviews customer servers to ensure properly documented exception requests. This process has been enhanced and a workflow developed within AST's ITSM system; however, AST must rely on customers to document any necessary exceptions.

Equally important, every customer also receives daily backup status reports that include not only every managed server backed up, but also the details of each job and the overall success rate. These reports

are sent to agency-specified distribution lists for internal review and verification that all intended servers are included in the backup rotation. Agency staff provide an additional means to monitor and verify that backups are appropriately scoped and successful.

Additional efforts at continuous improvements in the Backup and Recovery team process includes the development of an automated report of backup failures called the *Three-strike Report*. This report provides a list of every server that fails a backup for one, two, or three consecutive days within the Enterprise Backup System. The three-day failure is the highest priority for the team. The team generates tickets for this work every day to track each individual failure to ensure all work to remedy every failure is tracked to completion.

Of the six servers identified as not being backed up, three failed due to product failure, which is being addressed through replacement of the backup product; one was due to miscommunication that would have been discovered within existing backup audit controls; and two did not require backup but did not have appropriate documentation.

Another statement within the finding stated that:

> *Additionally, on October 20, 2017, we observed that a backup job within an AST backup system had been running continuously for 71 hours, thereby preventing other backup jobs from running. Upon audit inquiry, AST Backup Section staff stated that the backup job was for a daily backup that normally took 2 hours to complete. The Chief of Production System Services indicated that the staff person responsible for monitoring backups had been out sick for 3 days and no one had noticed the backup was still running and preventing other backup jobs.*

This backup job was within a separate legacy backup system and not part of the AST enterprise backup system. This separate backup server contains a very small number of backup clients and it was not included in the enterprise backup system's reporting capabilities or monitoring. Specialized and separate backup systems add risk by limiting the number of staff trained to address issues and by limiting integration into the enterprise monitoring and reporting processes. To address this risk, AST continues to focus heavily on eliminating separate isolated backup systems.

When managing backups for over 3,600 servers in the State Data Center and monitoring 13,000 to 14,000 backup jobs daily, there will always be backup failures and client issues, but the Backup and Recovery team have managed to maintain the required service target of a 95% success rate on a regular basis. Nonetheless, there is always room for improvement and the teams will continue to make continuous improvements to the Data Protection Service as evidenced above.

Finding # 8

Finding Title: Software Licensing

Platform: Interdepartmental Services

Finding Statement:

> The AST lacked policies and procedures for the management and monitoring of software licensing agreements. Such policies and procedures help prevent software licensing violations.

Recommendation:

We recommend that AST management complete the establishment of comprehensive policies and procedures related to the management and monitoring of software licensing agreements.

Program Response:

While AST administrative rule requires each agency to establish policies and procedures to manage and monitor the agency's regulatory, legal, risk, environmental and operational IT requirements, the rule does not provide a standard for which specific policies or procedures must be established, nor do they set a standard for the level of comprehensiveness. The intent of the AST rule was for agencies to identify agency-specific risks or requirements, and based on the judgement of the agency, to create policies and procedures to address them. AST maintains that it should have the latitude to determine the agency risk and establish policies and procedures accordingly.

Due to the extremely complex and highly specialized nature of software licensing[1], software license management is distributed throughout the agency based on platform expertise. It is only through the teams' diligence, expertise, and knowledge of the products and implementation models that compliance can be maintained. Further, simply monitoring agreements for compliance is not enough. As an IT service provider, AST has long realized that managing and monitoring software utilization is critical to achieving full control over cost (both license and maintenance cost).

To ensure that license thresholds are not exceeded, AST has undertaken continuous monitoring and improvements to controls for software licensing agreement management. These controls include configuration management of server deployments, scans of desktop and server installed software, administrative controls over desktops to prevent unauthorized downloads, annual review of software contracts, service request requirements for any software installations, and installed software annual true-ups. In addition, AST has successfully concluded direct license audits from multiple software vendors utilizing AST maintained records and resources. Any license reconciliations necessary were addressed within contractually available true-up processes.

AST is currently implementing a Software Asset Management tool that will address the entire lifecycle of software acquisition, deployment, and entitlement tracking. Once implementation is complete, AST plans to establish processes and procedures to ensure the appropriate use and maintenance of the tool. This tool will address the cited risk by automating the complex responsibility of compliance monitoring for AST and customer agencies.

---

[1] For example, the customer agencies have multiple versions of Microsoft SQL Server (SQL 2000, SQL 2005, SQL 2008, SQL 2010, SQL 2012, SQL 2016) in the SDC, running in different licensable configurations in multiple environments (development, test, production, training, staging, DR, etc.). There are standard version licenses, enterprise licenses, licenses by core, and by processor. There are embedded and OEM licenses, different versions have multiple, differing licensing requirements based the contract under which they were acquired or software assurance they are placed on, and each installation platform and each environment has different licensing restrictions.

Finding # 9

Finding Title: Performance Metrics

Platform: Central Services - Database

Finding Statement:

The State Data Center's monitoring and reporting of the performance metrics for database services provided to customer entities, as defined in service-level agreements, need improvement to ensure that critical incidents affecting the database services are timely detected, documented, and, as applicable, resolved.

Recommendation:

We again recommend that AST management ensure that SDC database performance uptime metrics included in the SLA agreements are met and that appropriate documentation for uptime performance statistics is maintained.

Program Response:

AST is compliant with the State law that states that the SDC is to establish in SLAs with customer entities the metrics and processes by which business standards for each service provided to the customer entities are to be objectively measured and reported.

The audit report states that there were no performance metrics in the monitoring tool for nine database instances. It did not establish that the metrics were not measured and reported, only that source data was not retained due to an issue that occurred during a monitoring product upgrade.

In order to ensure maintenance of metric data after future monitoring tool upgrades, the AST Oracle Database Platform modified its monitoring tool migration process to allow the old source monitoring tool to maintain the uptime data available for reporting for an additional year.

The report also states that the tickets provided for two of the four database instances reviewed did not provide sufficient detail to support the blackout period for scheduled maintenance. To address this issue, AST will include additional detail within the service requests for future maintenance events.

Lastly, AST will continue to monitor database performance to ensure that the established SLA performance metrics are met.

Finding # 10

Finding Title: Computer Security Incident Response Team

Platform: Office of Information Security

Finding Statement:

The AST's Computer Incident Response Team [CSIRT] processes need enhancement to promote prompt and appropriate responses to cybersecurity events.

Recommendation:

We recommend that AST management ensure that CSIRT meetings are conducted at least quarterly and that CSIRT members receive annual training as required by AST rules.

Program Response:

Corrective actions to address these findings regarding training and scheduled meetings have been completed. AST will continue to ensure that the CSIRT meetings and associated training occur in conjunction with requirements defined in rule.

Finding # 11

Finding Title: Security Controls – Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, Shared Accounts, Service Accounts, and Logging and Monitoring

Platform: Multiple / Platform Specific

Finding Statement:

Certain State Data Center security controls related to tape encryption, vulnerability management, configuration management, user authentication, shared accounts, service accounts, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of State Data Center customer entity data and related IT resources.

Recommendation:

We recommend that AST management improve certain security controls related to tape encryption, vulnerability management, configuration management, user authentication, shared accounts, service accounts, and logging and monitoring to ensure the confidentiality, integrity, and availability of SDC customer entity data and related IT resources.

Program Response:

As noted throughout the auditor's report, most of these issues were reported in the Auditor General's Report Number 2017-087. Several of these issues have long-term corrective action underway and would not be completed in under six months between the closing of Report Number 2017-087 and the start of this one.

AST will review the included security controls and implement corrective action, as determined appropriate.