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

MEMORANDUM

TO: Eric M. Larson, State Chief Information Officer/Executive Director
Eric Miller, Chief Inspector General, Executive Office of the Governor

FROM: Tabitha A. McNulty, Inspector General

DATE: September 28, 2018

SUBJECT: Six-Month Follow-up Status to the State of Florida Auditor General Report Number 2018-187, *Agency for State Technology, State Data Center Operations*

Pursuant to section 20.055, Florida Statutes, attached is the six-month status of findings and recommendations included in the Auditor General Report Number 2018-187, *Agency for State Technology, State Data Center Operations*, published March 29, 2018.

The agency continues to make progress on implementing the corrective actions and the associated long-term resolution efforts for recommendation implementation. The updates and status of the corrective actions are provided in the attached report under the sections Current Agency Status and Office of Inspector General (OIG) Assessment.

The overall results of the review found that sufficient corrective action was completed to close one recommendation. The OIG is also recommending that management accept any residual risk remaining on one recommendation since it is superseded by Internal Audit Report A-1617-36. The OIG will continue to follow-up on the remaining open recommendations.

If further information is needed, please contact me at 850-412-6022.

TAM

Attachment

cc: Kathy DuBose, Coordinator
Joint Legislative Audit Committee (JLAC)
Sherrill F. Norman, CPA
State of Florida Auditor General
Robert Thompson, Chief Operations Officer

Agency for State Technology
Office of Inspector General

Eric M. Larson, State CIO/
Executive Director

Tabitha A. McNulty
Inspector General

Six-Month Follow-up Response to *Agency for State Technology, State Data Center Operations* Auditor General Report Number 2018-187 Internal Audit Project # A-1819-12

Overview

Section 20.055, Florida Statutes, requires the Inspector General to monitor and report to the Executive Director and the Chief Inspector General on the status of corrective action taken in response to reports issued by the Auditor General. In March 2018, the Auditor General published Report Number 2018-187, *Agency for State Technology, State Data Center Operations*. This audit focused on evaluating selected information technology controls applicable to the operations of the State Data Center (SDC) during the period July 2016 through December 2017 and subsequent selected actions.

Status Report

Finding Number: 1 Disaster Recovery Planning

The State Data Center's 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.

Platform: Core Services – Disaster Recovery

Original Report Response (March 2017): 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.

Current Agency Status:

To ensure the DRP included all required elements, the AST initiated a review of the DR plan starting on April 18, 2018.

AST conducted a DRP test from May 7-11, 2018, that included all critical applications. After the DRP test any gaps in specific recovery processes or documentation was identified and updated, as necessary, to continually improve the process.

Office of Inspector General Assessment:

The Office of Inspector General (OIG) requested the updated DRP and results of the DRP testing several times for review. As of September 25, 2018, the documents were not provided and therefore, the OIG cannot confirm that the updates and that all critical applications were tested during the DRP test.

The OIG cannot make a determination as to the status of this finding and:

☒ will remain open. The OIG will follow-up in six months.
☐ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Finding Number: 2 Continuity of Operations Planning

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.

Platform: Core Services – Disaster Recovery

Original Report Response (March 2018): 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.

Current Agency Status:

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.

The updated ITSM workflow was implemented and a component of this workflow is to ensure the update of contact information in the IRIS. This process change helped to ensure that staff contact information is accurate and complete. Additionally, the IRIS system is being replaced which will provide more efficient updating of employee information and further ensure information remains up-to-date. The first test of the system was conducted on September 19, 2018. The new system includes staff notifications and requests acknowledgment of message receipt. The system also makes progressive notices instead of mass calls to all numbers at one time.

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. AST added informational links to the AST DRP into the AST COOP documents that include vital database information.

Office of Inspector General Assessment:

In Internal Audit Report A-1617-36, *Continuity of Operations Planning Process and Plan*, issued June 29, 2018, the OIG reviewed the issues noted in the Auditor General's reports and determined that the issue with employees not being in the IRIS system was not that they were not in the system, but that they were not showing up on the report that was provided to the audit staff. When the report was run for the entire population of people within IRIS, all of the employees missing were included. The IRIS administrator cannot explain why the missing employees did not appear on the initial report.

The OIG also noted that the COOP coordinator created a testing schedule that focused on the primary COOP elements: IRIS, Remote Desktop Gateway, and Virtual Desktop Infrastructure testing.

The OIG agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☐ is partially complete and will remain open. The OIG will follow-up in six months.

☐ is complete and the OIG will no longer follow-up on this.
☒ is not complete but recommends that management accept any residual risk. Additionally, with the issuance of Internal Audit A-1617-36, this finding is superseded.

Finding Number: 3 Inventory of IT Resources

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 [Configuration Management System Architecture] 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.

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

Original Report Response (March 2018): 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.

Current Agency Status:

AST is documenting 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 CMDB.

Additionally, the Director of Compliance, Risk, and Audit has implemented an audit remediation tracking process to ensure that corresponding remediation is being documented and tracked.

Office of Inspector General Assessment:

The OIG reviewed a draft of the document listing the various tools used to manage resources. Also, the OIG and the Director of Compliance, Risk, and Audit are in the process of implementing an off the shelf audit management product that includes audit remediation tracking process. Therefore, the OIG agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Finding Number: 4 Backup Tape Reconciliations and Destruction

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.

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

Original Report Response (March 2018): 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.

Current Agency Status:

AST collected tape data from the tape backup systems and compared to the list to the data in the tape tracking software. This information was then used to create a list of expired tapes that need to be destroyed. The tapes to be destroyed are located at disaster recovery site and AST is in the process of arranging for the tapes to be transported back to the SDC for destruction.

Additionally, Policy AST-BIOS-P-209, Tape Management is under revision and nearing finalization.

Office of Inspector General Assessment:

The OIG reviewed the draft policy and agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Finding Number: 5 Appropriateness of Access Privileges

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.

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

Original Report Response (March 2018): 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.

Current Agency Status:

AST is continuing to implement a privileged identity and access management system that will provide additional granularity for business function delegation. AST continue to work with customers to evaluate and verify that administrative accounts are appropriate and retain documentation evidencing approvals for the accounts.

The agency also continues to identify, document, and enhance platform specific processes that support ongoing appropriateness of access. The AST has also drafted an agency-wide Access Control Policy that is currently under review.

Additionally, AST continues to work with customer agencies to identify and remove unnecessary access and document delegations for accounts that need to be retained.

Office of Inspector General Assessment:

The OIG agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Finding Number: 6 Periodic Review of Access Privileges

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.

Platform: Windows; Central Services; Core Services

Original Report Response (March 2018): 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.

Current Agency Status

The Agency is evaluating the access reviews and making changes to further enhance access review processes. Additionally, an Access Control Policy has been drafted to communicate agency-wide expectations for managing access to IT resources.

Office of Inspector General Assessment:

The OIG reviewed the draft Access Control Policy and agrees with the status of the recommendation and determines that the finding:

- ☐ will remain open and the OIG will follow-up in six months.
- ☒ is partially complete and will remain open. The OIG will follow-up in six months.
- ☐ is complete and the OIG will no longer follow-up on this.
- ☐ is not complete but recommends that management accept any residual risk.

Finding Number: 7 Backup Controls

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.

Platform: Core Services – Backup and Recovery

Original Report Response (March 2018): 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.

Current Agency Status:

AST continues to migrate to a new backup system. Through this process the agency is ensuring that all required infrastructure is migrated and appropriately backed up. Also, since the issuance of report number 2018-187 and the new backup system implementation, AST has completed one customer backup audit and has 10 in process.

Office of Inspector General Assessment:

The OIG agrees with the current agency status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Finding Number: 8 Software Licensing

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.

Platform: Interdepartmental Services

Original Report Response (March 2018): 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.

Current Agency Status:

The Software Asset Management tool implementation projects continues to ingest and normalize installed software from all equipment under AST's control. Additionally, comprehensive documentation related to the management and monitoring of software licensing agreements is in draft and nearing finalization.

Office of Inspector General Assessment:

The OIG reviewed the draft of the Software Asset Management policy and agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

[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 Number: 9 Performance Metrics

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.

Platform: Central Services - Database

Original Report Response (March 2018): 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.

Current Agency Status:

Progress has been made in migrating databases to the new monitoring platform. Additionally, monitoring during the migration was implemented and is being maintained to ensure metrics are accurately calculated. Subsequent to the original response, a decision was made to not blackout monitoring during service requests. Blackouts instead only occur during the scheduled change and release events.

Office of Inspector General Assessment:

The OIG agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Finding Number: 10 Computer Security Incident Response Team

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.

Platform: Office of Information Security

Original Report Response (March 2018): 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.

Current Agency Status:

To ensure continued compliance with the requirements, the Agency has completed required CSIRT training, conducted three quarterly meetings for 2018, scheduled future CSIRT meetings, and tentatively scheduled the next training for November 2018.

Office of Inspector General Assessment:

This finding was corrected while the Auditor General's staff were onsite; therefore, the OIG agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☐ is partially complete and will remain open. The OIG will follow-up in six months.
☒ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

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

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.

Platform: Multiple / Platform Specific

Original Report Response (March 2018): 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.

Current Agency Status:

Corrective action to resolve some of the issues identified is complete. However, several of the remaining issues have long-term corrective action that are currently underway and will be monitored until complete.

Office of Inspector General Assessment:

The OIG agrees with the status of the recommendation and determines that the finding:

☐ will remain open and the OIG will follow-up in six months.
☒ is partially complete and will remain open. The OIG will follow-up in six months.
☐ is complete and the OIG will no longer follow-up on this.
☐ is not complete but recommends that management accept any residual risk.

Objective, Scope, and Methodology

The objective of this follow-up report was to determine the status of action taken by agency management in response to the findings and recommendations made in the Auditor General Report Number 2018-187. The review focused on corrective actions taken since the report's publication on March 29, 2018.

Items reviewed include:

- Draft AST policies and procedures,
- Documents and tickets concerning the periodic review of users and service accounts,
- Interviewing of employees involved in the remediation of audit issues.
- COOP plan and test results,
- Cherwell tickets including, change and release records, tape destruction, and incident reporting,

- Backup and recovery test and tape destruction documents
- Other security controls as noted in finding 11.

This work product was prepared pursuant to section 20.055, Florida Statutes, and is consistent with the applicable standards as defined in the Principles and Standards for Offices of Inspectors General (as published by the Association of Inspectors General) and International Standards for the Professional Practice of Internal Auditing (as published by The Institute of Internal Auditors, Inc.)

FLORIDA INSPECTORS GENERAL

ENHANCING PUBLIC TRUST

TRUST

To promote accountability, integrity, and efficiency in government, the Office of Inspector General conducts audits and reviews of Agency for State Technology's programs, activities, and functions.

Other reports prepared by the Office of Inspector General of the Agency for State Technology may be obtained by telephone (850-412-6022), mail (2585 Shumard Oak Blvd, Tallahassee, FL 32399), or by emailing Tabitha.McNulty@AST.MyFlorida.com