STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-149
March 2020

DEPARTMENT OF MANAGEMENT SERVICES

State Data Center Operations

Sherrill F. Norman, CPA
Auditor General

Head of the State Data Center and the State Chief Information Officer

During the period of our audit through June 30, 2019, the State Data Center was housed within the Agency for State Technology and the Executive Director of the Agency for State Technology served as the State's Chief Information Officer. Pursuant to Chapter 2019-118, Laws of Florida, effective July 1, 2019, the State Data Center and other functions of the Agency for State Technology were transferred to the Department of Management Services and the Division of State Technology was created. The Director of the Division of State Technology is appointed by the Department of Management Services Secretary and is the State Chief Information Officer.

Secretary of the Department of Management Services

The Department of Management Services is established by Section 20.22, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. The creation, powers, and duties of the Division of State Technology within the Department is established within Section 20.22(2)(b), Florida Statutes, and designates the Division's Director as the State Chief Information Officer. During the period of our audit from July 1, 2019, Jonathan Satter served as Department Secretary. The Division of State Technology Director position was vacant from July 1, 2019, through the end of our audit period.

Executive Director of the Agency for State Technology

The Agency for State Technology was established by Chapter 2014-221, Laws of Florida. The head of the Agency was the Executive Director. During the period of our audit through January 8, 2019, Eric Larson served as the Agency for State Technology Executive Director. The Executive Director position remained vacant from January 9, 2019, through the transfer of the Agency for State Technology to the Department of Management Services, effective July 1, 2019.

The team leader was Clark Evans, Jr., CPA, CISA, and the audit was supervised by Hilda S. Morgan, CPA, 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

DEPARTMENT OF MANAGEMENT SERVICES

State Data Center Operations

SUMMARY

This operational audit focused on evaluating selected information technology (IT) controls applicable to State Data Center (SDC) operations. The SDC operations were the responsibility of the Agency for State Technology (AST) during the period of our audit[1] through June 30, 2019, after which the SDC operations were transferred to the Department of Management Services and are housed within the Division of State Technology. This audit also included a follow up on the findings included in our report No. 2018-187 of the AST. Our audit disclosed the following:

Finding 1: The SDC's disaster recovery plan, annual testing, and processes for customers subscribing to the SDC disaster recovery services need improvement to ensure that critical SDC operations are recovered and continue in the event of a disaster or other interruption in service.

Finding 2: The SDC's continuity of operations plan continues 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: Inventory repositories for IT resources at the SDC were not complete and in some cases were not accurate, and configuration management database audits for servers were not performed, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated.

Finding 4: SDC processes for reconciling, tracking, and securing backup tapes need improvement to ensure that 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 users' assigned job responsibilities.

Finding 6: SDC processes for performance and documentation of periodic access reviews need improvement to ensure assigned access remains appropriate.

Finding 7: SDC backup controls continue to need improvement to ensure backups for all IT resources requiring backup are appropriately performed and periodically tested for recoverability to ensure that customer data is readily recoverable in response to an unexpected event.

Finding 8: SDC procedures and processes for the management and monitoring of software licensing agreements need improvement to help prevent software licensing violations.

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

[1] Our IT operational audit focused on evaluating selected IT controls applicable to SDC operations during the period July 2018 through November 2019 and selected actions subsequent thereto.

Finding 10: Certain SDC security controls related to logical access, tape encryption, vulnerability management, configuration management, user authentication, service accounts, and logging and monitoring, need improvement to ensure the confidentiality, integrity, and availability of 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, designated as the State Chief Information Officer, was responsible for, among other things, the management of the State Data Center (SDC). Pursuant to State law,[2] effective July 1, 2019, the AST was transferred to the Department of Management Services (Department) and, within the Department, the Division of State Technology (DST) was established.[3] The Director of the DST is appointed by the Department Secretary and is the State Chief Information Officer. Pursuant to State law,[4] Department 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 SDC.

According to State law,[5] the SDC's duties are to:

- Offer, develop, and support the 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 business continuity and disaster recovery plans, and annually conduct a live exercise of each 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.
- For SDC procurement processes, show preference for cloud-computing solutions that minimize or do not require the purchasing, financing, or leasing of SDC infrastructure, and meet the needs of customer agencies, reduce costs, and meet or exceed applicable State and Federal laws, regulations, and standards for IT security.
- Assist customer entities in transitioning from SDC services to third-party, cloud-computing services procured by the customer entities.

As shown in ***EXHIBIT A*** to this report, as of January 6, 2020, the SDC provided IT services to 31 customer entities that contract with the SDC for IT services. The 31 customer entities consisted of State agencies, a judicial branch entity, a county government, special districts, other governmental

[2] Chapter 2019-118, Laws of Florida.

[3] Section 20.22(2)(b), Florida Statutes.

[4] Section 282.0051, Florida Statutes.

[5] Section 282.201, Florida Statutes.

entities, and a nonprofit entity. The SDC provides to its customer entities a variety of IT 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.

FINDINGS AND RECOMMENDATIONS

Finding 1: Disaster Recovery Planning

Disaster recovery (DR) planning is intended to facilitate the timely recovery of critical applications, data, and services in the event of a disaster or other interruption in service. A business impact analysis (BIA) helps ensure that all critical applications, data, and services are identified for recovery. State law[6] requires the SDC, among other things, develop and implement a disaster recovery plan (DRP), and annually conduct a live exercise of the DRP. Additionally, State law[7] 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. Furthermore, Department rules[8] require that DRPs be tested at least annually, and that results of the annual exercise document the plan procedures that were successful and specify any modifications needed to improve the plan.

In prior audits of the AST, most recently in our report No. 2018-187, we noted that the SDC DRP and annual testing needed improvement to ensure that critical SDC operations were recovered and continued in the event of a disaster or other interruption in service. Our audit follow-up procedures disclosed that the SDC completed a live exercise of the SDC DRP on December 17, 2018, and updated the SDC DRP as of December 27, 2018. Our review of the exercise results report, SDC DRP, the service-level agreements (SLAs) for the 13 customer entities who contracted for SDC DR services, and other applicable records disclosed that:

- While the SDC DRP identified 20 critical SDC applications, the DRP did not contain sufficiently detailed step-by-step instructions for recoverability for 1 of the 20 applications, and the recoverability of the application was not tested during the December 2018 exercise or the prior DRP exercise conducted in May 2018. In response to our audit inquiry, SDC staff stated that this application was not deemed critical and, therefore, was removed from DR in late 2018, but the DRP was not updated. Also, a BIA was not conducted prior to the completion of the December 2018 update of the SDC DRP to determine the criticality of the applications for DR to ensure that all critical business functions were identified and could be resumed.
- SDC staff stated that, as of January 27, 2020, the SDC DRP had not been updated to incorporate necessary modifications identified for the testing completed on December 17, 2018, and a BIA still had not been conducted.
- For the recovery of the Open Systems environment, two sections, Restoration Results and Recovery Site and Evaluation Issues, were not documented in the DR exercise results report.
- Section 3 of the SDC DRP outlined the roles and responsibilities of the SDC and customer entities related to DR services for the customer entities and stated that the SDC was responsible for

[6] Section 282.201(1)(c), Florida Statutes.

[7] Section 282.201(1)(b), Florida Statutes.

[8] Department Rule 60GG-2.006(1)(e), Florida Administrative Code.

creating IT DRPs for customer entities that subscribed to SDC DR services. In response to our audit inquiry, SDC management stated that the requirement in the SDC DRP was inaccurate and that, although the SDC conducted customer entity DR exercises based on engagement documents, the SDC was not responsible or accountable for creating IT DRPs for customer entities subscribing to SDC DR services. SDC management further stated that copies of the customer entity IT DRPs were not maintained at the SDC and, therefore, would not be available to SDC staff in the event of an emergency. Our review of the SLAs for the 13 customer entities that contracted for SDC DR services found that detailed information related to the roles, responsibilities, and scope of DR services was not included in the SLAs. Similarly, the DR offering in the 2018-2019 Service Catalog did not include the roles and responsibilities of the SDC and the customer entities.

- As of November 14, 2019, full-scale testing or analysis to prepare for an event affecting the SDC and the 13 customer entities had not been performed to verify that the SDC had the necessary staff and infrastructure to meet the established recovery time objectives for each customer in the event of an outage affecting all customers.

We also reviewed the most recent customer entity DR exercise results reports, including engagement documents and other supporting documentation, for the 13 customer entities that subscribed to SDC DR services as of May 23, 2019. Our review disclosed that:

- For 3 customer entities, DR exercises were completed during our audit period, but the customer entity DR requirements for testing were not documented prior to the exercises. SDC staff stated that, while the DR exercises for these customer entities were conducted prior to implementing the use of engagement documents used to record DR testing requirements agreed upon by the SDC and the customer entity, no other documents were retained that established the DR testing requirements agreed upon with the 3 customer entities.
- The DR exercises completed for 2 customer entities, as described in the results reports, did not demonstrate timely recovery of all infrastructure. The report for 1 customer entity identified an issue on March 28, 2019, that was not resolved in the DR environment until April 25, 2019, and, as of January 10, 2020, the issue remained unresolved in the production environment. For the other customer entity, the SDC had not completed the configuration of a necessary storage infrastructure platform at the DR site; therefore, the data necessary for some of the testing was not available.

Completing a BIA to ensure the inclusion of all critical SDC applications in the DRP, providing step-by-step instructions for the recovery of each critical application in the DRP, conducting live exercises of the DRP, and modifying the DRP based on test results decrease the risk that critical SDC applications will not be timely and orderly resumed in the event of a disaster or other interruption of service. Accurate documentation of DR roles and responsibilities and testing requirements for customer entities, including documentation of the timely resolution of subsequently identified issues, and full-scale testing to prepare for an outage event affecting all customers, decrease the risk that critical customer entity applications and infrastructure will not be timely and orderly recovered in the event of a disaster or other interruption of service.

Recommendation: To ensure recoverability of the critical applications maintained at the SDC in the event of a disaster or other interruption of service, we recommend that Department management:

- **Conduct a BIA to identify all critical SDC applications and include step-by-step instructions in the DRP for each identified critical application.**

- **Conduct testing of all identified critical applications, evaluate and timely remediate issues identified in testing, and incorporate necessary DRP modifications identified during the testing.**
- **Accurately define the roles and responsibilities for customer entities that subscribe to DR services and ensure testing requirements are documented with the customer entities prior to DR testing.**
- **Timely evaluate and remediate customer entity DR testing results.**
- **Ensure full-scale testing is performed to verify that all applications and infrastructure can be timely restored for customer entities subscribing to DR services.**

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[9] requires the SDC to develop and implement a business continuity of operations plan (COOP) and annually conduct a live exercise of the plan. State law[10] 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.

The SDC maintains a COOP[11] with references to the SDC DRP for certain information. Our audit procedures disclosed that the SDC COOP needs improvement. Specifically:

- Although the SDC COOP referenced the SDC DRP and servers that contained databases supporting SDC critical applications were listed in the SDC DRP, the specific database names or other information identifying the vital databases were not included in either document.
- While the COOP referenced the SDC DRP that listed the critical applications and corresponding essential business functions, business functions were not listed for 3 of the 20 applications identified as critical.
- Neither the COOP nor the SDC DRP identified essential personnel.

In response to our audit inquiry, SDC management stated that, although the COOP had previously contained essential functions along with critical applications and personnel, the previous documentation was no longer necessary due to the use of remote desktop and virtual desktop technologies that allowed all staff to quickly and easily connect to required resources at any time. However, ease of access to resources is not a substitute for identification of essential functions and access to electronic resources may not always be available. SDC management also stated that they were in the process of creating a new policy to identify essential personnel; however, our review of the draft policy documentation

[9] Section 282.201(1)(c), Florida Statutes.

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

[11] Continuity of Operations Plan, AST Procedure CT004.

disclosed that a requirement for identifying the essential functions performed by SDC personnel was not included.

Identification in the SDC COOP of vital databases, business functions, and essential personnel would further promote the continuity of critical State functions and the availability of related information. Similar findings were noted in prior audits of the AST, most recently in our report No. 2018-187.

Recommendation: To promote the continued operations of the SDC, we recommend that Department management include in the SDC COOP, or incorporate by reference, all essential information specified in State law.

Finding 3: IT Asset Management

Effective IT asset management controls include the maintenance of a complete, accurate, and up-to-date inventory of IT resources (e.g., physical and virtual servers, network devices, databases, etc.) to ensure that management is knowledgeable of all IT resources for which they are responsible to facilitate the management of IT resources. Further, a complete, accurate, and up-to-date inventory is necessary for the effective monitoring, testing, and evaluation of IT resources and the timely implementation of the latest relevant security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors. Department rules[12] require each State agency to ensure that physical devices and systems within the organization are inventoried and managed.

The SDC maintained various repositories of the physical assets within the data center and a configuration management database (CMDB) of SDC-managed IT infrastructure and customer entity resources. As part of our audit, we evaluated SDC controls over the accuracy and completeness of the records of physical assets in the data center and configuration items (CIs) in the CMDB.

To determine whether the physical asset authoritative (primary) repository used to record the physical hardware devices in the data center was accurate and complete, we compared the inventory listing of 25 storage hardware devices from two storage array management systems (used to manage physical storage arrays in the data center) to the authoritative repository listing. Our comparison disclosed that the records in the authoritative repository listing for 5 of the 25 storage hardware devices were either missing or inaccurate. While SDC management provided additional information to help resolve the discrepancies in the repository, our search of the repository using the information provided either identified a different device or did not resolve the discrepancies.

According to SDC management, an annual reconciliation of the physical asset repository listing to the data center cabinets was performed to help maintain the accuracy of the inventory records for the physical assets in the data center. However, as of December 2, 2019, reconciliations had not been performed since March 2018 for the high-availability[13] floor and August 2017 for the fault-tolerant[14] floor. While SDC management performed a limited reconciliation in August 2018 for 10 selected fault-tolerant cabinets, our

[12] Department Rule 60GG-2.002(1)(a), Florida Administrative Code.

[13] High availability is the ability of a system or system component to be continuously operational for a desirably long length of time and is measured relative to 100 percent operational.

[14] Fault tolerant technology is the capability of a computer system, electronic system, or network to deliver uninterrupted service despite one or more of its components failing.

review of the physical asset repository inventory listing as of May 16, 2019, disclosed that over 300 cabinets were located in the data center. As a result, less than 4 percent of the inventory was reconciled. In response to our audit inquiry regarding the lack of reconciliations since 2018, SDC staff stated that only periodic checks of selected inventory for ongoing validation were performed because numerous processes exist to help ensure that inventory records are updated and verified and equipment does not enter or leave the data center without proper paperwork. However, as noted above, our audit procedures determined that records within the authoritative repository were not always complete and accurate.

The SDC recorded SDC-managed IT infrastructure and customer entity inventory items as CIs in the CMDB. The CIs included applications, databases, documents, network devices, storage items, servers, and other IT infrastructure items. In addition to descriptions of the CIs, the CMDB included the relationships between applications to servers and databases and other SLA-required metadata. The *Configuration Management Audit Procedures*[15] stated that 200 server CIs were required to be audited each fiscal year. Our review of the CMDB dashboard and exported data disclosed that only 115 server CI audits were completed during the 2018-19 fiscal year. In response to our audit inquiry, SDC management stated that an automated process for updating the CMDB audit records was disabled to troubleshoot another issue and was inadvertently left disabled for a period of time, preventing the CIs from linking to the audit records. As of August 12, 2019, the automated process was enabled to remediate the audit record linking problem and SDC staff were able to recover an additional 44 audit records for the fiscal year. Subsequently, SDC management indicated on November 22, 2019, that the procedure requiring the 200 audits was not formally approved; however, staff responsible for management of the CMDB stated that, as of January 8, 2020, they were continuing to follow the procedure and performing the audits of the CMDB.

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 evaluating of IT resources to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources. Similar findings were noted in prior audits of the AST, most recently in our report No. 2018-187.

Recommendation: To ensure the accuracy of IT asset records, we recommend that Department management continue efforts to establish a complete, accurate, and up-to-date inventory of all SDC-managed hardware, perform annual reconciliations of the repository for physical assets to the data center cabinets, and complete the CMDB configuration audits annually.

Finding 4: Backup Tape Reconciliations and Destruction

Department rules[16] require the mirroring, or creation of regular backups of current copies, of data and software essential to the continued operation of critical agency functions with storage at an off-site location. Effective backup controls include policies, procedures, and processes to ensure that accurate records of the location and status of backup data are maintained and that all backup tape media is accounted for, allowing an entity to minimize the risk of data loss that may occur as a result of unexpected

[15] AST Procedure CF006.

[16] Department Rule 60GG-2.006(1)(b), Florida Administrative Code.

events. Such actions facilitate the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

Our audit procedures disclosed that reconciliation and off-site storage and tracking controls for backup tape media need improvement. Specifically:

- While SDC procedures[17] required a semiannual reconciliation of the backup systems that created the tapes to the tape tracking system used to record the movement of tapes between the SDC and the off-site storage vendor, a reconciliation was not performed during the period July 1, 2018, through November 30, 2019. In response to our audit inquiry, SDC management indicated that the required reconciliation was not performed because Backup and Recovery Section staff thought changes to tape processes removed the need to perform the reconciliation and reports necessary to perform the reconciliation were no longer available. However, after further research, SDC staff determined the reports were available and the reconciliation can be resumed.
- According to SDC management, tape reconciliation processes included SDC staff conducting a semiannual inspection at the off-site storage location to verify the location of all tapes listed in the tape tracking system as located at the off-site storage location. Our examination of the records for the inspection conducted in the fall of 2018 disclosed that the complete tape inventory at the off-site storage location was not reconciled as the inspection was limited to approximately 8,900 tapes that were being destroyed. SDC management indicated that a full reconciliation of the records in the tape tracking software to the inventory at the off-site storage location was completed on August 2, 2019.
- Our physical inspection of backup tapes at the off-site storage location on June 11, 2019, disclosed 149 fewer tapes than were indicated by the location records in the tape tracking system. Vendor staff at the off-site storage location indicated that SDC staff had taken 98 backup tapes to the SDC on June 6, 2019; however, the removal of the tapes was not recorded in the tape tracking system. SDC procedures require staff to record the movement of tapes in the tape tracking system prior to movement. In response to our audit inquiry, SDC management indicated that the tapes were retrieved at the request of the SDC customer entity whose data resided on the tapes and that, while the 98 tapes were retrieved from the off-site location on June 6, 2019, the tape tracking records were not updated until after the tapes were returned to the SDC. A reason for the remaining discrepancy of 51 tapes was not provided.

We also evaluated whether appropriate approvals and records of destruction were maintained for 46 of the 11,537 backup tape records marked in the tape tracking system as destroyed as of May 16, 2019. Our audit procedures, including inquiries of SDC staff, disclosed that 2 of the 46 tapes had not been physically destroyed as indicated in the tape tracking system. In response to our audit inquiry, SDC management stated that, while 1 of the 2 tapes was not destroyed, the tape could not be located as of August 2, 2019, after a physical inspection of the tapes in the vault at the off-site storage location. For the other tape, SDC management stated the tape was renumbered in the tape tracking system and the original tape number should have been removed from the tape tracking system rather than marked as destroyed.

Complete and timely periodic reconciliations of backup tape records and inspections of backup tapes at the off-site storage location improve the ability of management to demonstrate that appropriate accountability and control of backup tapes is maintained. In addition, accurate tape records improve the SDC's ability to locate backup tapes and timely and completely recover information in the event of a loss

[17] Tape Management and Reconciliation Procedure, AST-BIOS-P-0209.

of production data. Also, complete and accurate approval and documentation of tape destruction improves the SDC's ability to demonstrate that appropriate accountability and control of backup tapes has been maintained and unauthorized access to confidential or exempt information has been prevented. Similar findings were noted in prior audits of the AST, most recently in our report No. 2018-187.

Recommendation: We recommend that Department management ensure that semiannual reconciliations of the backup systems that create backup tapes to the tracking system used to record the movement of tapes to the off-site storage location are performed as specified in Department procedures and documented. In addition, tape tracking system records should periodically be compared to the physical tape inventory at the off-site storage location. We also recommend that Department management ensure that tape location records are timely updated 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 users' assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

State law[18] requires the SDC to assume administrative access rights to resources and equipment, including servers, network components, and other devices, consolidated into the SDC. State agencies are to relinquish administrative rights to consolidated resources and equipment and the SDC is to provide customer entities with access to applications, servers, network components, and other devices necessary for entities to perform business activities and functions.

As part of our audit, we evaluated administrative access privileges to the mainframe, Windows server, and Oracle database environments, and the interconnected network domains. Our audit procedures disclosed user accounts with administrative access privileges to mainframe environment resources that were not assigned to SDC staff. In response to our audit inquiry, SDC management stated the accounts were assigned to customers for administration of the customers' resources. However, SDC staff were unable to demonstrate as of September 16, 2019, that SDC staff had certified the accounts and related privileges remained necessary and appropriate. Specifically, we noted that:

- For the Resource Access Control Facility (RACF) mainframe security environment applicable to three logical partitions (LPARs)[19] assigned to one State agency, 20 of the 35 active accounts with one or more administrative access authorities were assigned to the State agency's staff as of April 26, 2019. The administrative access authorities included the ability to copy, reorganize, catalog, scratch user or data sets, specify logging options, and have full control over all RACF user profiles.
- For the CA Top Secret mainframe security environment applicable to one State agency's LPAR, 1 of the 7 active administrative accounts with unlimited scope privileges as of May 2, 2019, was assigned to State agency staff. This account had the ability to create a terminal session.

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

[19] 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 instance of an operating system.

Our audit procedures also disclosed server accounts with administrative access privileges that were not appropriate. Specifically, for 33 of the 2,263 Windows production servers, 22 of the 183 accounts in the local *Administrators* group managed by the SDC as of August 7, 2019, were not necessary.

Our evaluation of the 47 administrative access accounts for 6 of the 20 Oracle production database clusters as of July 11, 2019, disclosed that 20 of the 47 administrative accounts were not assigned to current SDC staff. In response to our audit inquiry, SDC management indicated that the administrative accounts required analysis to determine whether the accounts were necessary and that, as part of an ongoing effort to remove unnecessary accounts with excessive permissions, database administration staff were working with the respective customer entities to ensure the accounts could be removed.

Additionally, our audit procedures disclosed the existence of user accounts with administrative access as of April 12, 2019, on three of the six SDC-managed network domains[20] that were not appropriate, including active administrative user accounts assigned to employees who had separated from employment. Specifically, as shown in Table 1, 7 of the 163 active accounts with administrative access were not appropriate.

Table 1
Inappropriate Network Administrative Access Privileges

	Number of Accounts with Administrative Access Privileges on an SDC-Managed Domain		
Network Domain	**Total Administrative Accounts**	**Inappropriately Assigned to SDC Staff**	**Access Assigned to Former Employees**
1	52	1	2
2	74	-	1
3	37	2	1
Total	**163**	**3**	**4**

Two of the 4 accounts assigned to former employees were assigned to one individual and, as of April 12, 2019, the 4 accounts assigned to the 3 former employees had remained active from 71 to 308 days after the employees' separation dates.

Inappropriate and unnecessary administrative access privileges to the mainframe, Windows server, and Oracle database environments, and the interconnected network domains, increase the risk of unauthorized modification, loss, or disclosure of data and IT resources. Similar findings were noted in prior audits of the AST, most recently in our report No. 2018-187.

Recommendation: To promote compliance with State law and an appropriate separation of duties, we recommend that Department management properly restrict administrative access privileges to the mainframe, Windows servers, and Oracle database environments, and the interconnected network domains, to only those functions necessary for the user's assigned job responsibilities and ensure administrative accounts are timely disabled when no longer necessary.

[20] 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.

Finding 6: Periodic Review of Access Privileges

Department rules[21] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. An effective periodic review consists of identifying the current logical and physical access privileges of all users and evaluating the assigned access privileges to ensure that they align with users' job responsibilities.

Our audit procedures disclosed that the periodic access privilege review processes performed by the SDC need improvement. Specifically:

- In response to our request for documentation of periodic reviews performed for Windows server local administrative and Active Directory administrative accounts, SDC management stated that in accordance with *Active Directory Account Audit Procedure*,[22] periodic reviews of some administrative accounts were initiated using a scheduled task that ran a script biweekly in all SDC domains. The script generated a report of administrative access for each domain and automatically converted the reports to service requests requiring staff review. The reviewer created a change ticket for any account requiring changes (e.g., disabling). Our examination of the reports disclosed that:
    - Reports generated on March 25, 2019, and August 12, 2019, for two domains did not contain all administrative accounts for the respective domains. According to SDC management, the script only reported the *Enterprise*, *Schema*, and *Domain Admins* security groups for Active Directory and did not include the *Administrators* security group. SDC management further stated that reports were not generated, nor access reviewed, for Windows server local administrative accounts.
    - 1 of the 20 active accounts listed on the report dated March 25, 2019, was for an employee who had separated from AST employment on January 31, 2019. The biweekly reviews were ineffective as the account remained active and was not discovered during four biweekly reviews, including the review of the report generated on March 25, 2019.
- Although SDC management responsible for Oracle access within the Database Section of the Bureau of Central Services reviewed the access of current staff members within the Bureau on a periodic basis, not all active accounts, including accounts assigned to customer entities, were evaluated. In response to our audit inquiry, SDC management stated that customer entity user and application accounts were managed by the customers and were not reviewed by the SDC. Notwithstanding, as of November 25, 2019, SDC staff had not established ownership of all active accounts to ensure that all noncustomer accounts were included in the SDC review.
- SDC management responsible for open systems access within the Open Systems Section of the Bureau of Central Services performed a quarterly review of access privileges granted to Open Systems Section staff. Reports were generated individually for each employee within the Open Systems Section with assigned server access. The reviews were not comprehensive as accounts on some servers could be omitted because the reviews were not performed on a server by server basis and did not encompass administrative accounts within the service management system assigned to others, including other SDC staff, customers, or historical accounts from prior data center administrations.

[21] Department Rule 60GG-2.003(1)(a)6., Florida Administrative Code.

[22] AST-BWS-AP-0001.

As part of our audit, we also evaluated the *Physical Access Control Procedure*[23] and *Employee Action Procedure*[24] and related process for periodic reviews of physical access privileges to the SDC buildings. The *Physical Access Control Procedure* required reviews of access be initiated in March and September of each year. The procedure further stated that supervisors would receive a notice to review access, including access to SDC buildings, according to the process details documented in the *Employee Action Procedure*. We found that periodic reviews of assigned physical access privileges were performed for staff with unlimited access privileges to the data center facility; however, periodic reviews were not performed for SDC staff with limited access privileges to the data center facility or for Department staff with access to the Sadowski Building. In response to our audit inquiry, SDC management stated that, although a periodic review was not performed, all badge requests were submitted by supervisors through the ticketing system, which served as documentation of a review.

Without documented effective processes for performing comprehensive reviews of logical and physical access privileges using complete access lists, management's assurance that user access privileges were properly authorized and remain appropriate is limited.

Recommendation: We recommend that Department management perform comprehensive periodic reviews of logical and physical access privileges for users, maintain documentation of the reviews conducted, and ensure that access privileges are timely removed when no longer needed.

Finding 7: Backup Controls

State law[25] requires the SDC to ensure proper data backup and data recovery. According to the SLAs,[26] the Data Protection Service provides scheduled backups of customer entity data contained within the SDC and on supported, managed, or co-located operating systems within the designated backup window. In addition, Department rules[27] require State agencies to ensure that backups of information are conducted, maintained, and tested.

Our review of backup procedures performed on May 20, 21, and 22, 2019, for 48 of the 2,229 production Windows and Red Hat Enterprise Linux physical and virtual servers disclosed that SDC backup controls need improvement. As similarly noted in prior audits of the AST, most recently in our report No. 2018-187, we found that the SDC had not successfully completed the required daily backups for 5 of the 48 selected servers. Specifically:

- For 1 server, the SDC was unable to demonstrate that the server was backed up on any of the 3 days evaluated. In response to our audit inquiry, SDC management stated the server was decommissioned in 2016 and recommissioned in 2017; however, the status in the CMDB was not revised when the server was recommissioned and, therefore, as of May 22, 2019, the server had not been backed up since it was recommissioned. According to SDC staff, the server was subsequently added to the backup process on June 4, 2019.

[23] AST-BIOS-P-100.

[24] AST-ED-P-0021.

[25] Section 282.201(1)(b), Florida Statutes.

[26] 2018-2019 Service Catalog, Attachment A, Data Protection Service.

[27] Department Rule 60GG-2.003(5)(d), Florida Administrative Code.

- Although 4 other servers were subject to the backup process, the SDC was unable to demonstrate that daily backups were performed for the servers on all 3 days evaluated. Three of the 4 servers were successfully backed up for 2 of the 3 days but no backup occurred for the fourth server on any of the 3 days evaluated. In response to our audit inquiry, SDC management stated that the backup system in question only retained logs for 3 days and the incomplete backups were not investigated during that time frame, so the reason for the incomplete backups was unknown.

In our report No. 2018-187, Finding 7, we also reported that a backup job within one of the backup systems ran continuously for 71 hours unnoticed. As part of our follow-up procedures we inquired of SDC management as to whether any manual or automated systems were in place to notify staff when a backup task for the legacy backup systems was not completing within a reasonable time frame. In response to our audit inquiry, SDC management stated that no manual or automated process was in place to detect abnormally long-running backup tasks.

While SDC policy[28] required annual data recoverability testing, our audit procedures disclosed that, as of July 16, 2019, the SDC had not performed annual testing of data backups for recoverability since 2017. In response to our audit inquiry, SDC management stated data backups had not been tested for recoverability because the task was overlooked as a result of staff changes. On July 17, 2019, SDC management stated that restoration testing procedures had been documented, an automated task had been created to notify staff to perform annual testing starting in April 2020, and the restoration testing for 2019 was in progress. Subsequently, SDC management indicated in August 2019 that the restoration testing for 2019 was completed.

Timely, complete, and successful data backups and testing of data backups for recoverability help ensure that customer entity data is readily recoverable and available when needed in response to unexpected events.

Recommendation: We recommend that Department management ensure that all required server backups are timely and successfully performed, legacy backup systems are monitored to help ensure backup tasks are timely and successfully completed, and backups are periodically tested for recoverability.

Finding 8: Software Licensing

Department rules[29] require each agency to establish policies and procedures to manage and monitor the agency's operational requirements based on the agency's assessment of risk. Documented 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.

In our report No. 2018-187, Finding 8, we noted that the AST lacked comprehensive policies and procedures for the management and monitoring of software licensing. Our follow-up procedures found that the AST established a Software Asset Management Project Management Plan in February 2018 and implemented a software asset management policy[30] in January 2019. However, a project for the

[28] Backup and Recovery Policy, AST-BCOS-P-0007.

[29] Department Rule 60GG-2.002(3), Florida Administrative Code.

[30] Software Asset Management Policy, AST-ED P-0044.

identification, procurement, and implementation of a software asset management solution (software asset management registry tool) with an estimated project completion date of January 4, 2019, had not been completed as of February 6, 2020. For example, the initial import of software license data related to installation, deployment, and entitlement into the software asset management registry tool had not been completed. Also, procedures to define the software asset management processes for software entitlement entry in, and maintenance of, the registry and periodic monitoring for compliance had not been completed as of December 9, 2019. In response to our audit inquiry, Department staff indicated that, due to shifting resources and the anticipated transition activities impacting internal processes, resources, and the potential scope of the project and procedures, a completion date for the project was unknown.

A complete and up-to-date software asset management registry and comprehensive procedures and processes for managing and monitoring software license agreements decreases the risk of violations of such agreements.

Recommendation: We recommend that Department management promptly complete the software asset management project and finalize procedures for managing and monitoring 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,[31] the SDC is to establish in 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. Additionally, the *AST Overview of Oracle Service Standards and Policies* requires all Oracle database host servers to be monitored 24 hours a day, 7 days a week, by the Oracle monitoring system, the primary monitoring tool. The SLAs require Oracle database uptime of a minimum of 99.5 percent of the monthly scheduled availability for each respective database and a minimum uptime of 99.5 percent for Network Services.

Our audit procedures included evaluating the SDC's achievement of targeted performance metrics for uptime for both the production Oracle databases and the network. Our review of the performance metrics for 14 of the 59 production Oracle databases utilized by nine selected State agency customers during the period July 1, 2018, through May 31, 2019, disclosed that the SDC did not always meet its monthly performance target. Specifically, according to the reported performance metrics, the SDC did not meet its monthly performance target for three (the Department of Elder Affairs, Department of Management Services, and Department of Revenue) of the nine selected State agency customers for at least 1 month during the above time frame, as the Oracle database uptime for 1 of each customer's databases was less than 99.5 percent of the scheduled availability.

Additionally, for seven production Oracle databases for five State agency customers we found that the primary monitoring tool did not accurately reflect database performance during the period July 1, 2018, through May 31, 2019. In response to our audit inquiry, SDC management stated that for two databases

[31] Section 282.201(1)(d)5., Florida Statutes.

(both for Department of Transportation), reporting inaccuracies resulted from a failed software migration to a more recent version of the primary monitoring tool. For another database (for Department of Elder Affairs), SDC management stated that reporting inaccuracies resulted from the monitoring agent being nonfunctional due to issues with a legacy operating system. For the other four databases (one each for the Department of Children and Families, Department of Economic Opportunity, Department of Elder Affairs, and Department of Management Services), SDC management stated that blackout periods (database downtime due to maintenance) were overstated, and that, although maintenance was performed, the blackout status was not timely removed from the monitoring tool by SDC database staff.

Our review of performance metrics reported in the primary monitoring tool that measures network services uptime at the SDC and inquiries of SDC management regarding the methodology used to measure network services uptime for SDC State agency customers disclosed that, while the SDC monitors the availability of all network devices, only the network devices impacting all State agency customers (network devices common to all State agency customers) were included in the network availability statistics. According to SDC management, all State agency customers received the same report of network services uptime and the network uptime reported did not reflect discrete measurements of the uptime of all network devices utilized by each customer. In response to our audit inquiry, SDC management stated that only 10 network devices impacting all agency customers were measured and included in the availability metrics for network services for each month during the 11-month period July 2018 through May 2019. An additional 10 network devices were added in June 2019 for a total of 20 devices in the measurement for the month of June 2019. This method of calculating network services uptime based only on selected network devices common to all State agency customers could provide an inaccurate measurement for customers who may be impacted if 1 of the network devices that is not common to all customers is down and renders the network unavailable.

Notwithstanding the limitations related to the measurement of network services uptime, we reviewed the network services uptime records for the 12-month period July 2018 through June 2019. Our review disclosed that the number of network devices included in the uptime records provided to us was not consistent for each month during that period. In response to our audit inquiry, SDC staff stated that a recent software update to the monitoring tool resulted in a loss of network services performance monitoring records. Although SDC staff successfully retrieved monthly availability data for all network devices included in the report to SDC agency customers for the months of December 2018 through June 2019, no data was available for July 2018 and, as shown in Table 2, the availability data was incomplete for the 4-month period August 2018 through November 2018. As a result, we were unable to determine the accuracy of the monthly network services uptime calculated by the SDC.

Table 2

Number of Devices Included in the Network Services Uptime Measurement

Month	Number of Devices Reported
August 2018	5
September 2018	4
October 2018	2
November 2018	2

In response to our audit inquiry, SDC management stated that the software update to the monitoring tool that resulted in the loss of network performance monitoring records was discovered on March 15, 2019, and, at that time, data could only be retrieved from the monitoring tool back to December 2018.

Effective database and network performance monitoring are essential to the timely detection and resolution, as applicable, of critical incidents involving database and network services. Additionally, without complete records, the SDC cannot demonstrate the accuracy of reported uptime statistics or compliance with the SLA performance metrics. Similar findings were noted in prior audits of the AST, most recently in our report No. 2018-187.

Recommendation: We recommend that Department management ensure that SDC database performance uptime metrics included in the SLAs are met, appropriate documentation for uptime performance statistics is maintained, and network services performance uptime metrics reflect all SDC-managed network devices used by each customer entity.

Finding 10: Security Controls – Logical Access, Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, 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 SDC security controls related to logical access, tape encryption, vulnerability management, configuration management, user authentication, service accounts, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising customer entity data and related IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to logical access, tape encryption, vulnerability management, configuration management, user authentication, 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 were communicated to AST management, most recently in connection with our report No. 2018-187.

Recommendation: We recommend that Department management improve certain security controls related to logical access, tape encryption, vulnerability management, configuration

management, user authentication, service accounts, and logging and monitoring to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report No. 2018-187 of the AST.

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 February 2019 through November 2019 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 IT controls applicable to State Data Center (SDC) operations during the period July 2018 through November 2019 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, all deficiencies disclosed in audit report No. 2018-187 of the AST.
- 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 IT systems and 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 Department personnel and obtained an understanding of the organizational structure, statutory requirements, key policies, procedures, and operational processes for the Division of State Technology (DST) 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, network components, and database management systems.
- Obtained an understanding of the SDC services offered, customer entities served, and the division of responsibilities between the SDC and the customer entities.
- Evaluated the SDC's compliance with contractual requirements for performance uptime monitoring for the Oracle databases and the interconnected network infrastructure. Specifically, we reviewed:
  - The monthly performance metrics for 14 of the 59 stand-alone Oracle databases in production for the period July 1, 2018, through May 31, 2019, to evaluate whether the SDC met its monthly uptime performance metric, and whether the monitoring utility accurately reflected database performance.
  - The network services uptime calculation methodology and the measurement records for the network services monthly uptime performance for the period July 1, 2018, through June 30, 2019.
- Evaluated the effectiveness of SDC policies, procedures, and processes for vulnerability management including analysis and remediation of reported vulnerabilities for the SDC network, mainframe, Windows, and open systems environments.
- Evaluated the adequacy of the SDC's IT resource inventory tracking processes. Specifically, we compared:
  - Records for 40 of the 497 active open systems servers listed in the patch management system to the open systems server inventory repository as of June 3, 2019.
  - Records for 40 of the 2,225 active Windows servers listed in the configuration management database (CMDB) to the Windows server inventory repository as of July 11, 2019.
  - The 8 uniquely-named high-risk physical network devices listing a serial number in a network monitoring tool to the physical asset inventory tracking system as of May 16, 2019.
  - For 2 storage array device types, records for the 25 storage hardware devices listed in their applicable storage array management system to the physical asset inventory tracking system as of May 16, 2019.

  - For 1 storage system, records for the 6 backup storage hardware devices housed at the SDC to the physical asset inventory tracking system as of May 16, 2019.

- Evaluated the adequacy of the processes for ensuring the accuracy of the records in the CMDB. Specifically, we reviewed records for the 159 inventory items within the CMDB audited during the period July 1, 2018, through June 30, 2019.
- Evaluated the effectiveness of SDC configuration management policies, procedures, and processes for servers and network devices including patch management. Specifically, we reviewed:
  - 16 high-risk network devices to evaluate whether, as of June 7, 2019; June 10, 2019; and June 25, 2019, the SDC timely installed vendor-supplied patches.
  - 43 of the 264 Red Hat Enterprise Linux production open systems servers to evaluate whether, as of June 21, 2019, the SDC had timely installed vendor-supplied patches.
  - 39 of the 667 Windows production servers running one of two selected operating system versions to evaluate whether, as of July 16, 2019, the SDC had timely installed a vendor-supplied patch addressing a critical vulnerability.
- Evaluated the effectiveness of SDC logging and monitoring controls.
- Evaluated SDC continuity of operations and disaster recovery plans and determined whether the SDC had conducted a live exercise of each plan as required by Section 282.201(1)(c), Florida Statutes.
- Evaluated SDC disaster recovery processes for State agency customer entities subscribing to SDC disaster recovery services.
- Evaluated the effectiveness of SDC backup policies, procedures, and processes, including daily server backups, backup media recoverability testing, backup tape reconciliations, off-site tape storage, and tape destruction. Specifically, we:
  - Examined daily backup reports for 48 of the 2,229 Windows and Red Hat Enterprise Linux production servers as of May 22, 2019, to determine whether required backups were performed.
  - Evaluated periodic reconciliations performed of backup tape records to ensure backup tape media location records remain accurate and complete.
  - Evaluated whether annual recoverability testing of selected backup media had been performed.
  - Evaluated whether backup tape media was securely stored off-site and location records were accurately maintained.
  - Examined tape destruction records for 46 of the 11,537 tape records with a destroyed status as of May 16, 2019, to determine whether accurate documentation of approvals and destruction records were maintained.
- Evaluated tape encryption procedures and processes and reviewed records of the monthly audits performed for 30 selected backup tapes for May 2019.
- Evaluated selected administrative accounts for legacy backup systems to determine whether they were secured.
- 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 for the 6 network domains used for SDC services and operations as of April 12, 2019.
- The appropriateness of access privileges for the 183 accounts with administrative access privileges to their respective Windows servers as of August 7, 2019, on 33 of the 2,263 Windows production servers.
- The appropriateness of access privileges for the 43 active Resource Access Control Facility (RACF) administrative accounts with one or more selected elevated access authorities assigned across four logical partitions (LPARs) as of April 26, 2019.
- The appropriateness of access privileges for the 34 active Access Control Facility 2 (ACF2) administrative accounts with one or more selected elevated access privileges for 1 mainframe LPAR as of April 26, 2019.
- The appropriateness of access privileges for the 7 CA Top Secret administrative accounts with unlimited scope for 1 mainframe LPAR as of May 2, 2019.
- The appropriateness of access privileges for 38 administrative accounts on 43 of the 264 open systems servers as of June 21, 2019.
- The appropriateness of access privileges for 6 of the 20 production Oracle database clusters as of July 11, 2019.
- The adequacy of periodic review procedures for logical access privileges for the Windows, mainframe, network, open systems, and Oracle database environments.

- Evaluated the effectiveness of SDC IT infrastructure user authentication controls. Specifically, we reviewed:
  - RACF user authentication controls for 5 mainframe LPARs as of April 26, 2019.
  - ACF2 user authentication controls for 1 mainframe LPAR as of April 26, 2019.
  - CA Top Secret user authentication controls for 1 mainframe LPAR as of May 2, 2019.
  - User authentication controls for 43 of the 264 Linux Red Hat production servers as of June 21, 2019.
  - User authentication controls for 12 selected high-risk network devices as of June 7, 2019; June 10, 2019; and June 14, 2019.
  - User authentication controls for 6 of the 20 Oracle production cluster databases as of July 11, 2019.
  - User authentication controls for the 6 network domains used for SDC services and operations as of April 12, 2019.
- Evaluated the adequacy of the policies, procedures, and processes for the management and monitoring of software licensing at the SDC.
- Evaluated whether the policies, procedures, and processes for incident response were sufficient including the establishment of a Computer Security Incident Response Team in compliance with Department rules to respond to cybersecurity threats.
- Reviewed the processes at the SDC for monitoring and accurately reporting the status of corrective actions to remediate audit findings.
- Evaluated the adequacy of SDC policies and processes for authorizing, removing, periodically reviewing, and logging of physical access to the SDC data center facility and Sadowski Building including evaluating the 32 key cards with unlimited access to the SDC data center facility as of April 12, 2019.

- Evaluated whether adequate guidelines and processes were in place for governance and operational oversight of infrastructure procurement related to capacity planning and anticipated customer utilization, and whether operational oversight was effective in ensuring only necessary procurements occurred.
- 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

Sherrill F. Norman, CPA
Auditor General

EXHIBIT A

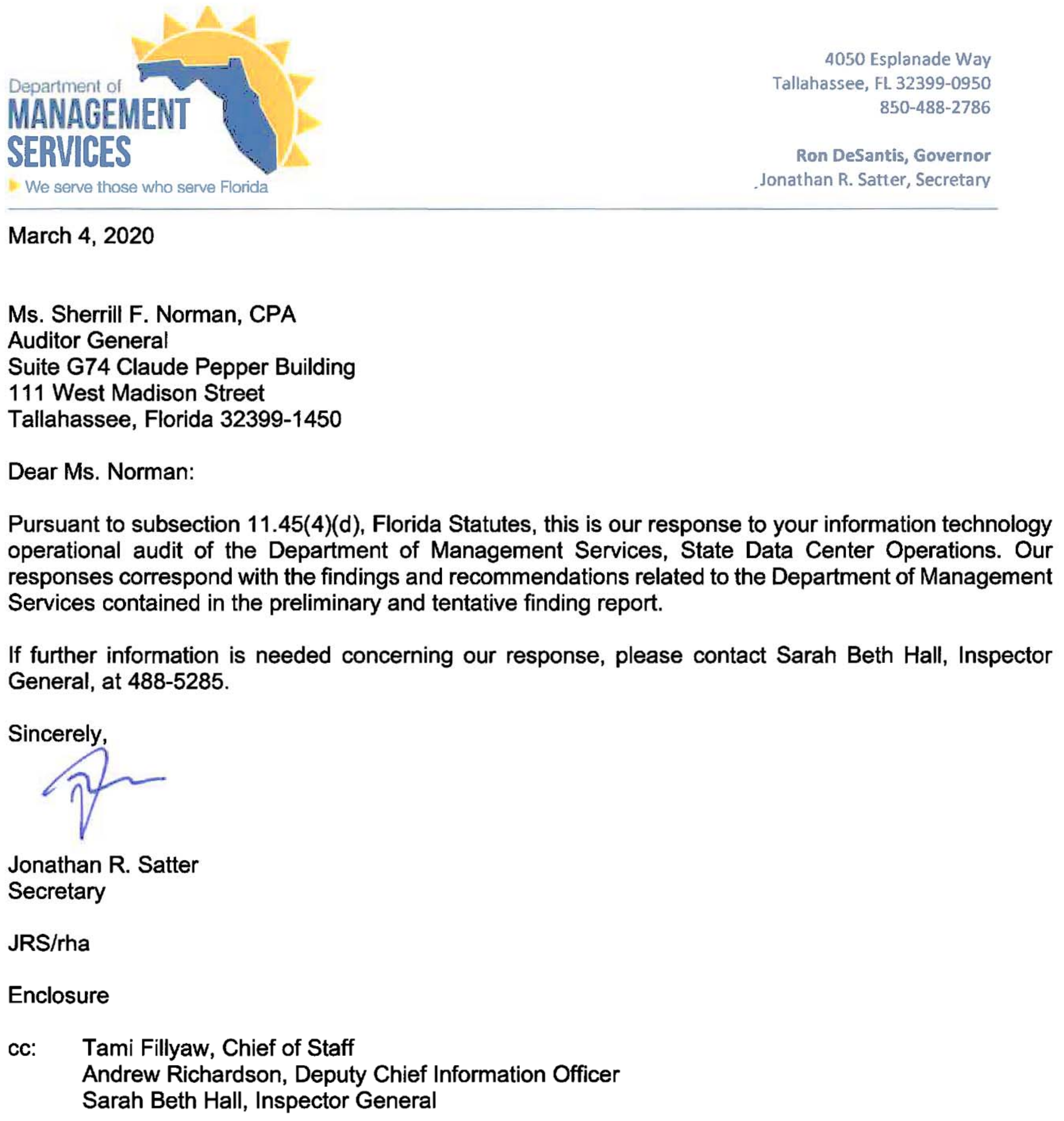
LIST OF STATE DATA CENTER CUSTOMER ENTITIES

AS OF JANUARY 6, 2020

	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 the 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 Fish and Wildlife Conservation Commission
25	Greater Orlando Aviation Authority
26	Justice Administrative Commission
27	Miami-Dade Expressway Authority
28	Northwest Florida Water Management District
29	Public Employees Relations Commission
30	Public Service Commission
31	Santa Rosa County

Source: Department records.

MANAGEMENT'S RESPONSE



Department of
MANAGEMENT
SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
850-488-2786

Ron DeSantis, Governor
Jonathan R. Satter, Secretary

March 4, 2020

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

Dear Ms. Norman:

Pursuant to subsection 11.45(4)(d), Florida Statutes, this is our response to your information technology operational audit of the Department of Management Services, State Data Center Operations. Our responses correspond with the findings and recommendations related to the Department of Management Services contained in the preliminary and tentative finding report.

If further information is needed concerning our response, please contact Sarah Beth Hall, Inspector General, at 488-5285.

Sincerely,

Jonathan R. Satter
Secretary

JRS/rha

Enclosure

cc: Tami Fillyaw, Chief of Staff
Andrew Richardson, Deputy Chief Information Officer
Sarah Beth Hall, Inspector General

Finding 1

Disaster Recovery Planning

Finding:

The SDC's disaster recovery plan, annual testing, and processes for customers subscribing to the SDC disaster recovery services need improvement to ensure that critical SDC operations are recovered and continue in the event of a disaster or other interruption in service.

Recommendation:

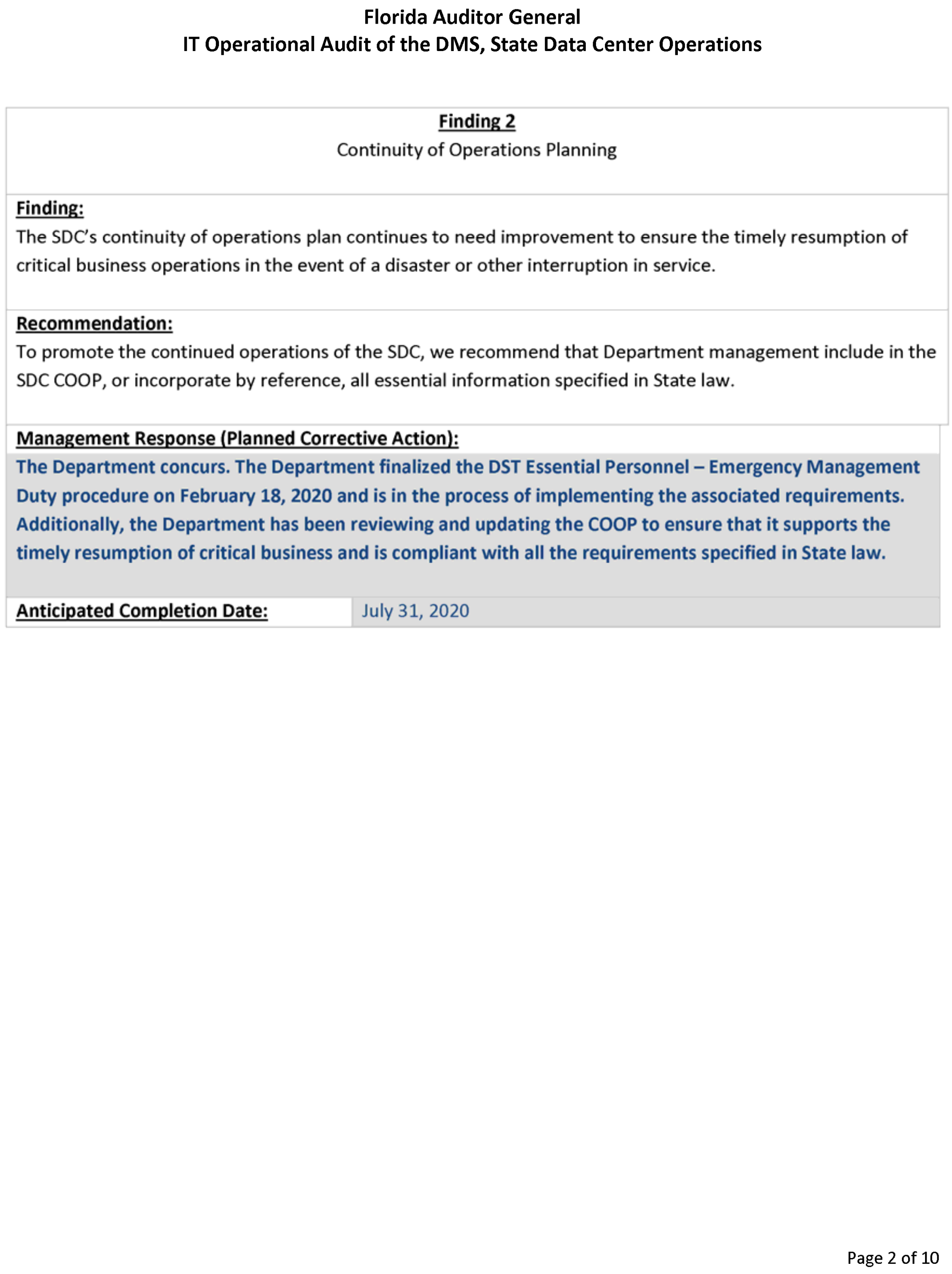
To ensure recoverability of the critical applications maintained at the SDC in the event of a disaster or other interruption of service, we recommend that Department management:

- Conduct a BIA to identify all critical SDC applications and include step-by-step instructions in the DRP for each identified critical application.
- Conduct testing of all identified critical applications, evaluate and timely remediate issues identified in testing, and incorporate necessary DRP modifications identified during the testing.
- Accurately define the roles and responsibilities for customer entities that subscribe to DR services and ensure testing requirements are documented with the customer entities prior to DR testing.
- Timely evaluate and remediate customer entity DR testing results.
- Ensure full-scale testing is performed to verify that all applications and infrastructure can be timely restored for customer entities subscribing to DR services.

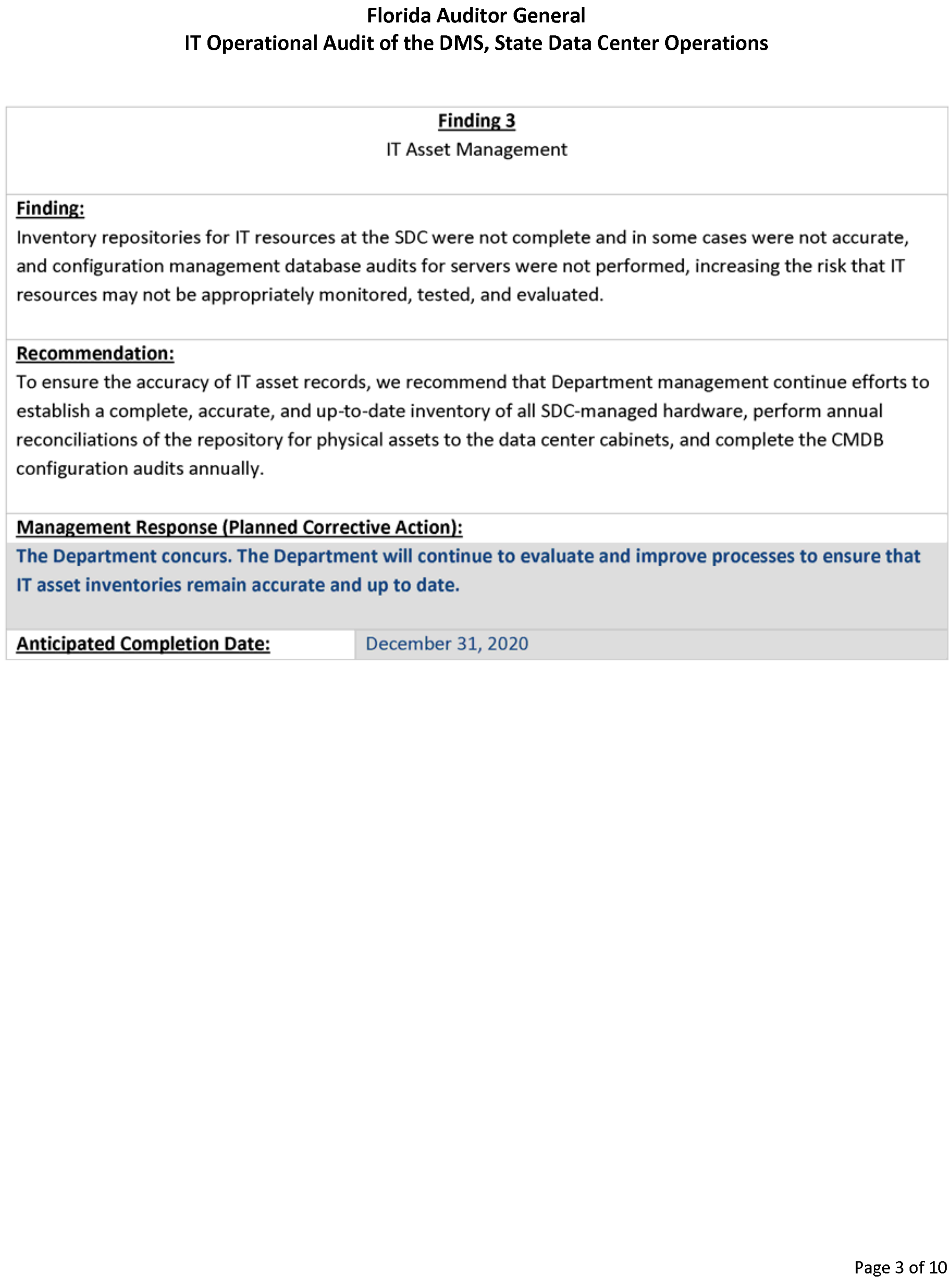
Management Response (Planned Corrective Action):

The Department concurs. The Department is currently implementing changes to the CMDB which will address the gap in the BIA process. Additionally, the Department is in the process of updating the service catalog and DR plan to accurately reflect the roles and responsibilities of the customer and data center. Although the Department has not conducted a single full-scale test of DR, annual customer testing is conducted to ensure timely restoration. The Department will continue to evaluate and improve DR testing to ensure that it is comprehensive, remedial, and appropriately documented.

Anticipated Completion Date:	February 28, 2021



Finding 2 Continuity of Operations Planning	
Finding: The SDC's continuity of operations plan continues 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 promote the continued operations of the SDC, we recommend that Department management include in the SDC COOP, or incorporate by reference, all essential information specified in State law.	
Management Response (Planned Corrective Action): **The Department concurs. The Department finalized the DST Essential Personnel – Emergency Management Duty procedure on February 18, 2020 and is in the process of implementing the associated requirements. Additionally, the Department has been reviewing and updating the COOP to ensure that it supports the timely resumption of critical business and is compliant with all the requirements specified in State law.**	
Anticipated Completion Date:	July 31, 2020



Florida Auditor General
IT Operational Audit of the DMS, State Data Center Operations

Finding 3
IT Asset Management

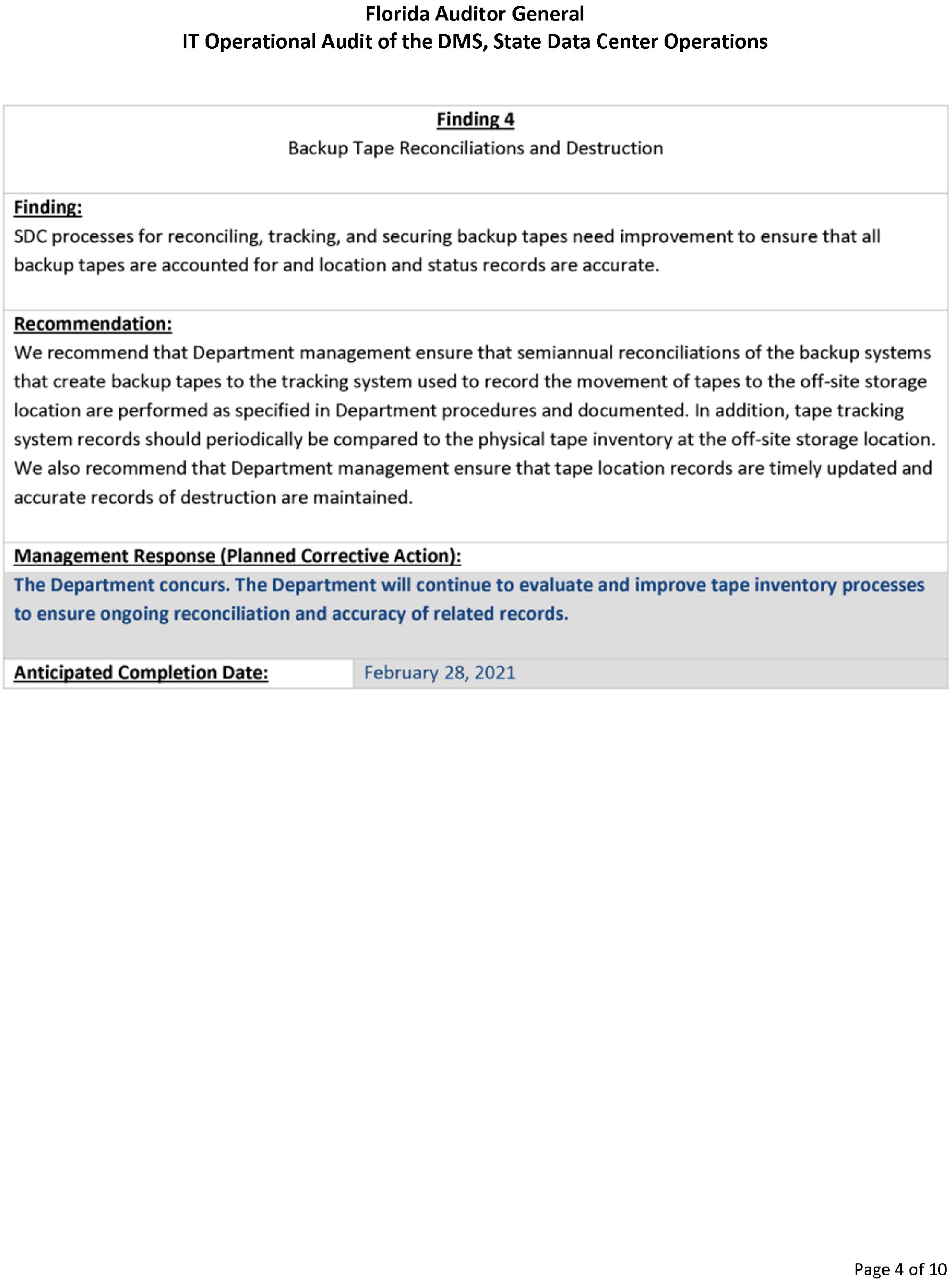
Finding:
Inventory repositories for IT resources at the SDC were not complete and in some cases were not accurate, and configuration management database audits for servers were not performed, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated.

Recommendation:
To ensure the accuracy of IT asset records, we recommend that Department management continue efforts to establish a complete, accurate, and up-to-date inventory of all SDC-managed hardware, perform annual reconciliations of the repository for physical assets to the data center cabinets, and complete the CMDB configuration audits annually.

Management Response (Planned Corrective Action):
The Department concurs. The Department will continue to evaluate and improve processes to ensure that IT asset inventories remain accurate and up to date.

Anticipated Completion Date:	December 31, 2020

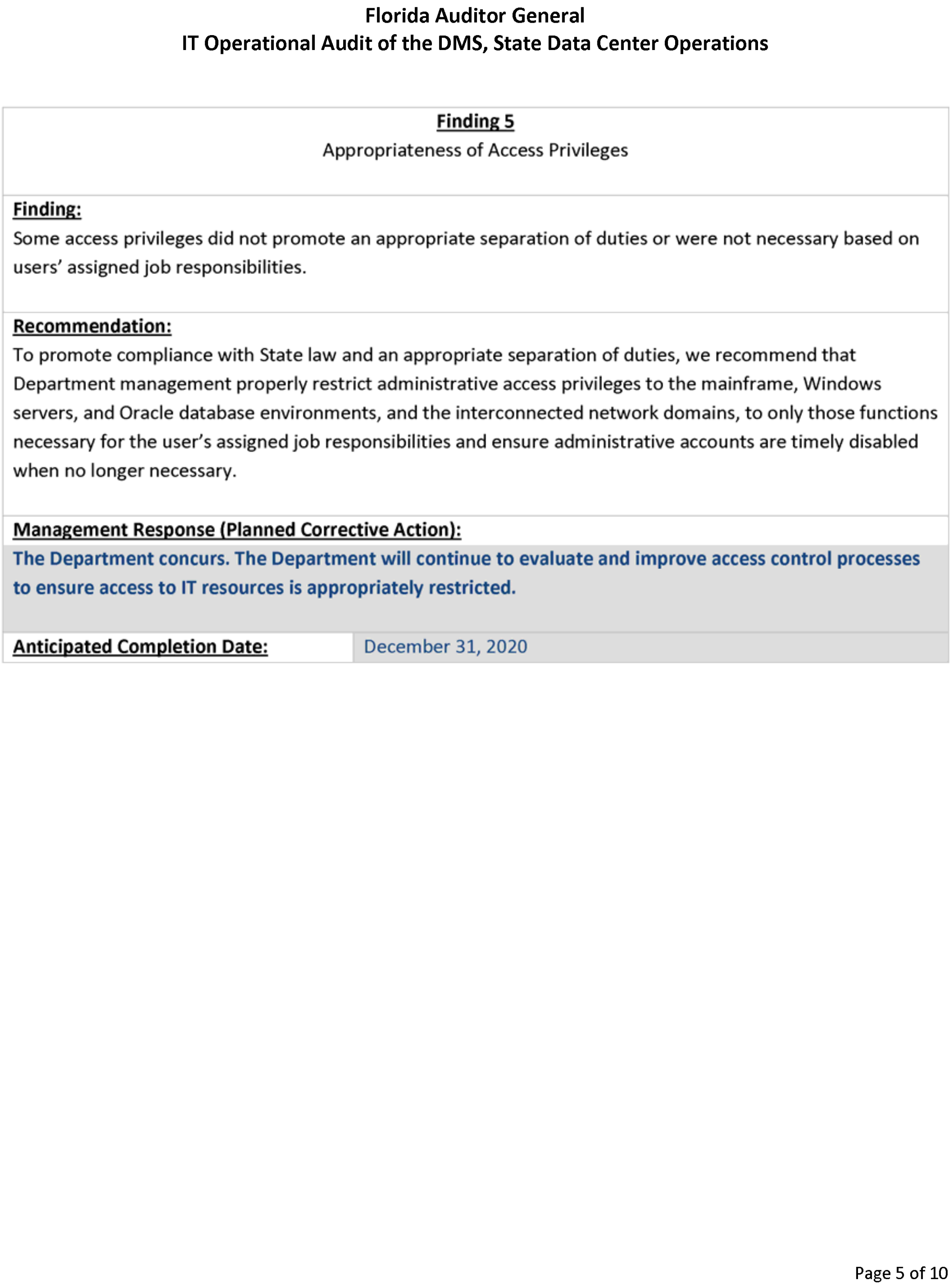
Page 3 of 10



Florida Auditor General
IT Operational Audit of the DMS, State Data Center Operations

Finding 4 Backup Tape Reconciliations and Destruction	
Finding: SDC processes for reconciling, tracking, and securing backup tapes need improvement to ensure that all backup tapes are accounted for and location and status records are accurate.	
Recommendation: We recommend that Department management ensure that semiannual reconciliations of the backup systems that create backup tapes to the tracking system used to record the movement of tapes to the off-site storage location are performed as specified in Department procedures and documented. In addition, tape tracking system records should periodically be compared to the physical tape inventory at the off-site storage location. We also recommend that Department management ensure that tape location records are timely updated and accurate records of destruction are maintained.	
Management Response (Planned Corrective Action): **The Department concurs. The Department will continue to evaluate and improve tape inventory processes to ensure ongoing reconciliation and accuracy of related records.**	
Anticipated Completion Date:	February 28, 2021

Page 4 of 10



Finding 5

Appropriateness of Access Privileges

Finding:

Some access privileges did not promote an appropriate separation of duties or were not necessary based on users' assigned job responsibilities.

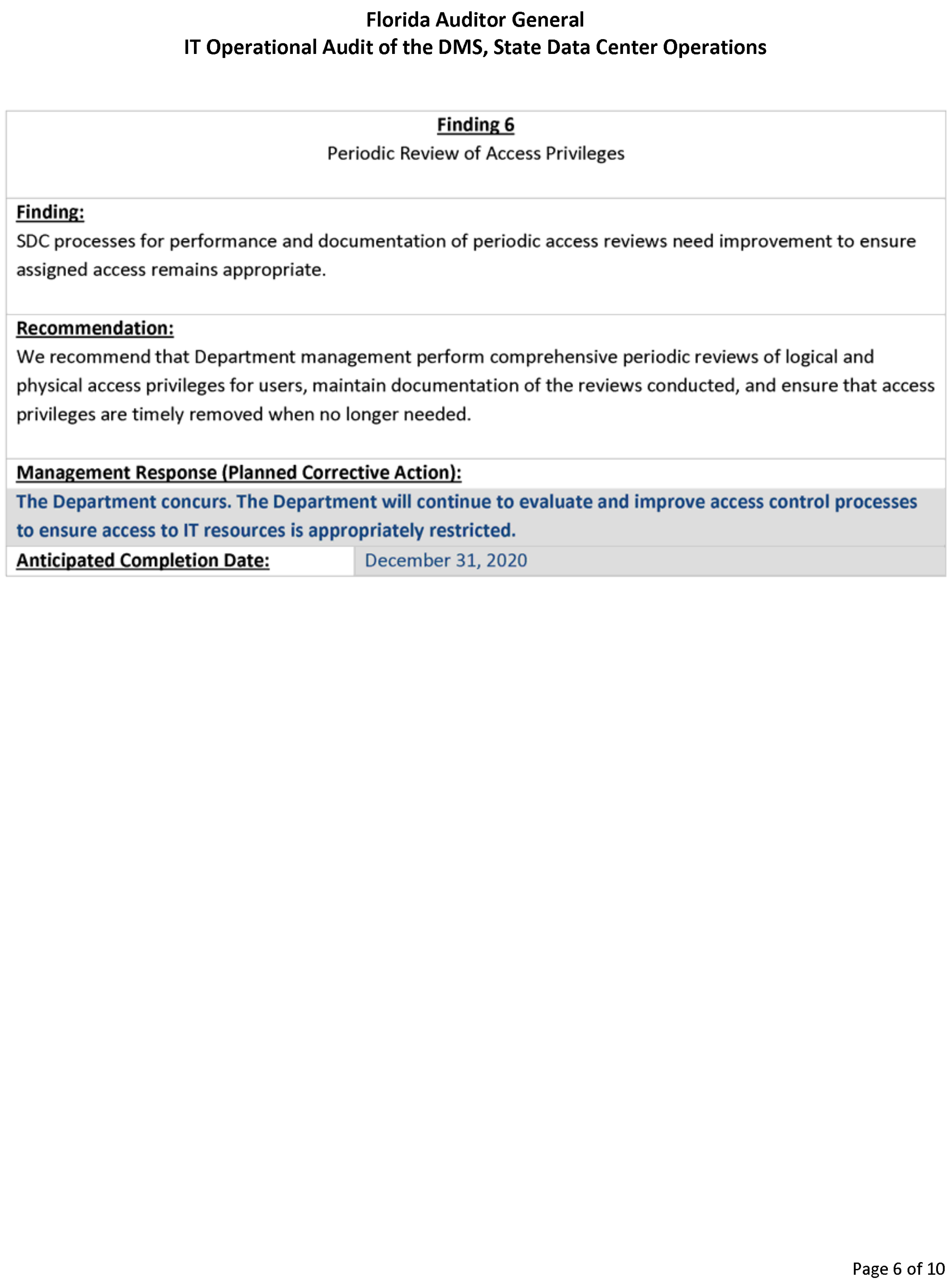
Recommendation:

To promote compliance with State law and an appropriate separation of duties, we recommend that Department management properly restrict administrative access privileges to the mainframe, Windows servers, and Oracle database environments, and the interconnected network domains, to only those functions necessary for the user's assigned job responsibilities and ensure administrative accounts are timely disabled when no longer necessary.

Management Response (Planned Corrective Action):

The Department concurs. The Department will continue to evaluate and improve access control processes to ensure access to IT resources is appropriately restricted.

Anticipated Completion Date:	December 31, 2020



Finding 6

Periodic Review of Access Privileges

Finding:

SDC processes for performance and documentation of periodic access reviews need improvement to ensure assigned access remains appropriate.

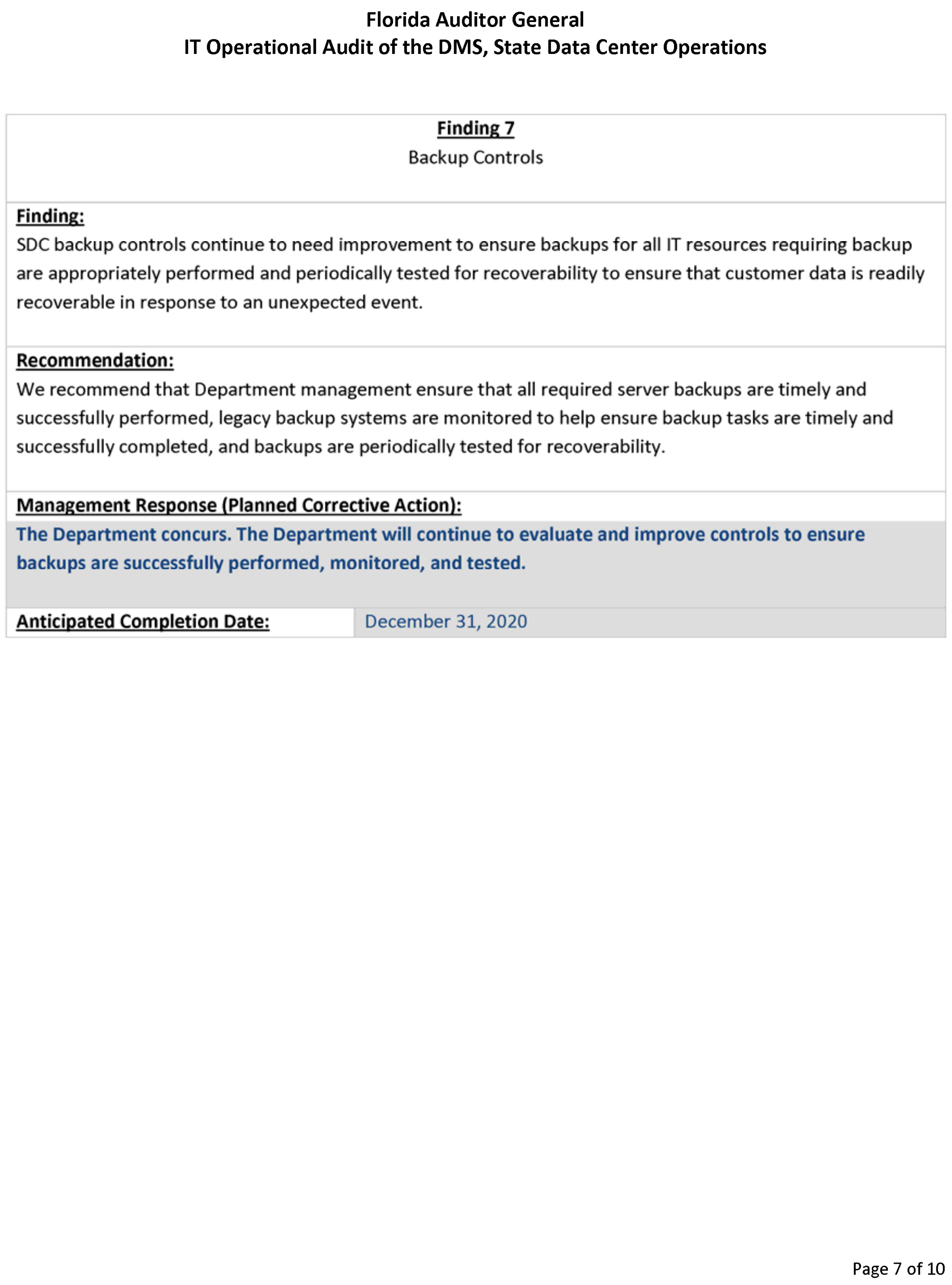
Recommendation:

We recommend that Department management perform comprehensive periodic reviews of logical and physical access privileges for users, maintain documentation of the reviews conducted, and ensure that access privileges are timely removed when no longer needed.

Management Response (Planned Corrective Action):

The Department concurs. The Department will continue to evaluate and improve access control processes to ensure access to IT resources is appropriately restricted.

Anticipated Completion Date:	December 31, 2020



Finding 7

Backup Controls

Finding:

SDC backup controls continue to need improvement to ensure backups for all IT resources requiring backup are appropriately performed and periodically tested for recoverability to ensure that customer data is readily recoverable in response to an unexpected event.

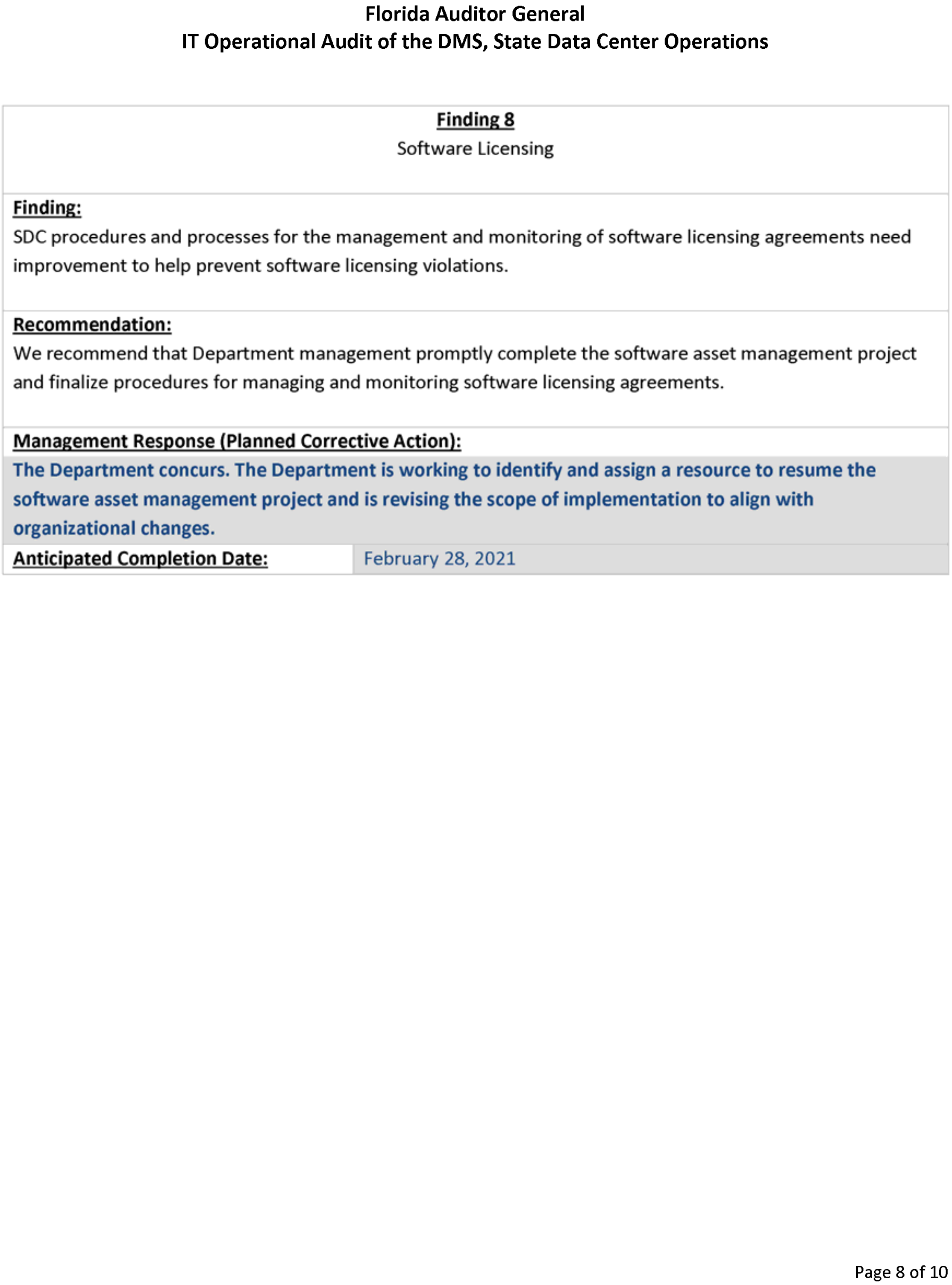
Recommendation:

We recommend that Department management ensure that all required server backups are timely and successfully performed, legacy backup systems are monitored to help ensure backup tasks are timely and successfully completed, and backups are periodically tested for recoverability.

Management Response (Planned Corrective Action):

The Department concurs. The Department will continue to evaluate and improve controls to ensure backups are successfully performed, monitored, and tested.

Anticipated Completion Date:	December 31, 2020



Finding 8

Software Licensing

Finding:

SDC procedures and processes for the management and monitoring of software licensing agreements need improvement to help prevent software licensing violations.

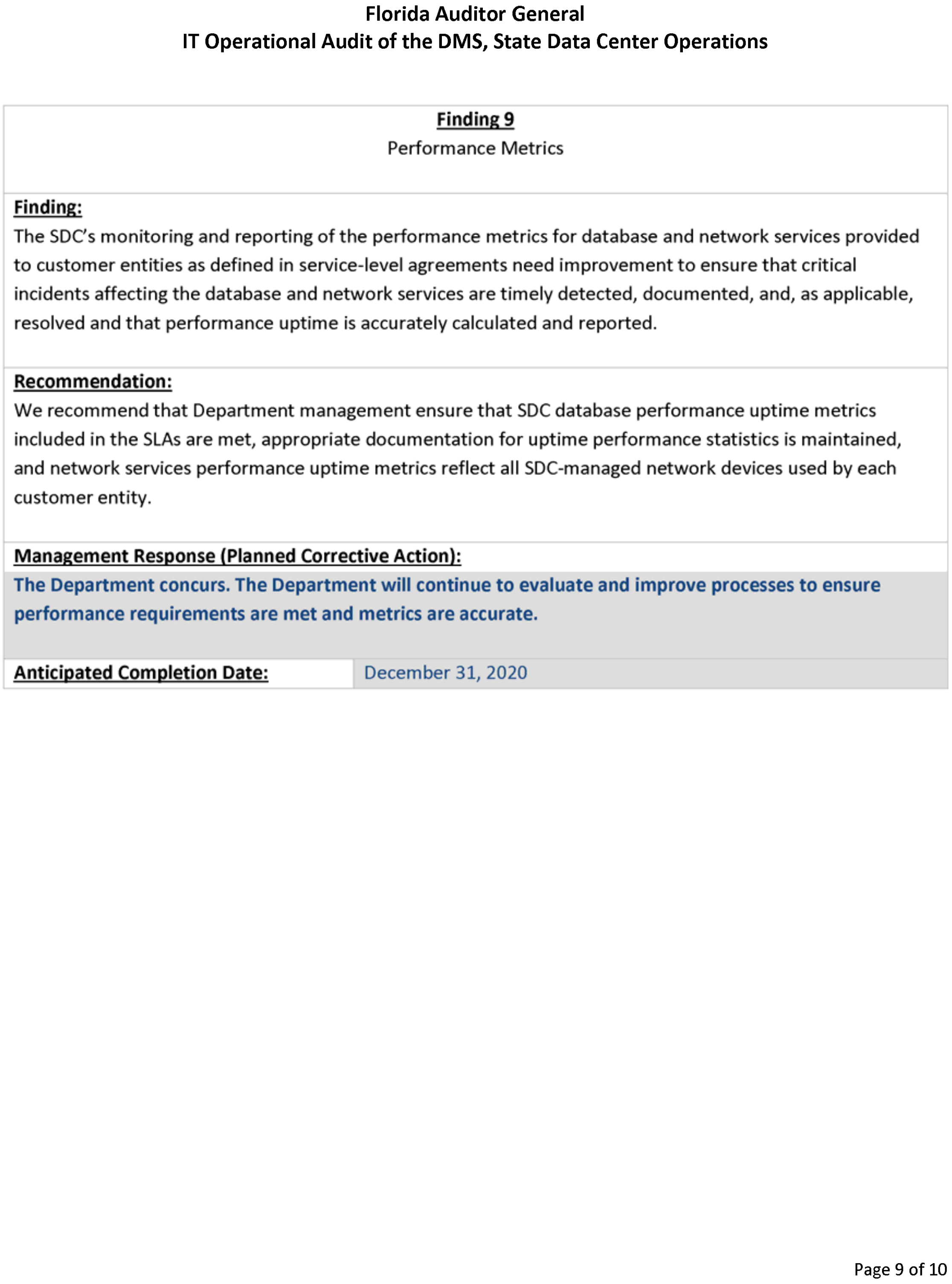
Recommendation:

We recommend that Department management promptly complete the software asset management project and finalize procedures for managing and monitoring software licensing agreements.

Management Response (Planned Corrective Action):

The Department concurs. The Department is working to identify and assign a resource to resume the software asset management project and is revising the scope of implementation to align with organizational changes.

Anticipated Completion Date:	February 28, 2021



Finding 9

Performance Metrics

Finding:

The SDC's monitoring and reporting of the performance metrics for database and network services provided to customer entities as defined in service-level agreements need improvement to ensure that critical incidents affecting the database and network services are timely detected, documented, and, as applicable, resolved and that performance uptime is accurately calculated and reported.

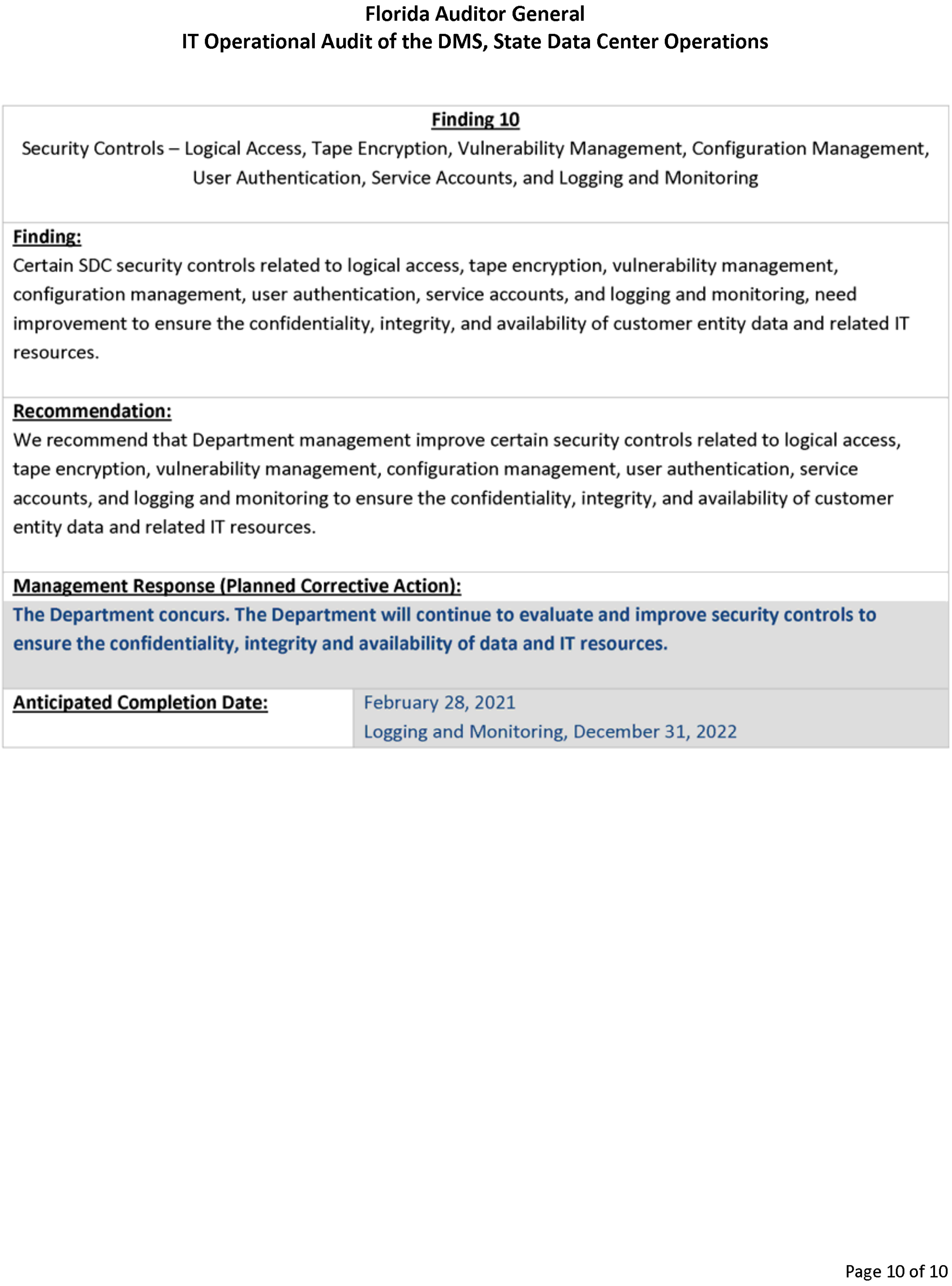
Recommendation:

We recommend that Department management ensure that SDC database performance uptime metrics included in the SLAs are met, appropriate documentation for uptime performance statistics is maintained, and network services performance uptime metrics reflect all SDC-managed network devices used by each customer entity.

Management Response (Planned Corrective Action):

The Department concurs. The Department will continue to evaluate and improve processes to ensure performance requirements are met and metrics are accurate.

Anticipated Completion Date:	December 31, 2020



Florida Auditor General
IT Operational Audit of the DMS, State Data Center Operations

Finding 10

Security Controls – Logical Access, Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, Service Accounts, and Logging and Monitoring

Finding:

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

Recommendation:

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

Management Response (Planned Corrective Action):

The Department concurs. The Department will continue to evaluate and improve security controls to ensure the confidentiality, integrity and availability of data and IT resources.

Anticipated Completion Date:	February 28, 2021 Logging and Monitoring, December 31, 2022

Page 10 of 10