STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-179
March 2022

DEPARTMENT OF MANAGEMENT SERVICES

State Data Center Operations

Sherrill F. Norman, CPA
Auditor General

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. During the period of our audit, the following individuals served as Secretary:

J. Todd Inman	From June 30, 2021[a]
Jonathan Satter	Through February 12, 2021

[a] Position was vacant February 13, 2021, through June 29, 2021.

The team leader was Clark Evans, CPA, CISA, and the audit was supervised by Brenda Shiner, CISA.

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

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

FLAuditor.gov

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

State of Florida Auditor General

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

DEPARTMENT OF MANAGEMENT SERVICES

State Data Center Operations

SUMMARY

This operational audit of the Department of Management Services (Department) focused on evaluating selected information technology (IT) controls applicable to State Data Center (SDC) operations. The audit also included a follow-up on the findings included in our report No. 2020-149. Our audit disclosed the following:

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

Finding 2: As similarly noted in prior audits, most recently in our report No. 2020-149, SDC continuity of operations plan documentation did not include all essential information specified in State law.

Finding 3: SDC processes for reconciling backup tapes were insufficient to ensure that all backup tapes were accounted for and backup records were accurate.

Finding 4: As similarly noted in our report No. 2020-149, SDC processes for performing and documenting periodic access reviews for the network, Windows server, open systems, and Oracle database environments did not adequately ensure that assigned access privileges remained appropriate.

Finding 5: SDC backup controls continue to need improvement to ensure that backups for all IT resources requiring backup are appropriately performed and documented.

Finding 6: The SDC's monitoring and reporting of the performance metrics for database services provided to customer entities continue to need improvement to ensure that critical incidents affecting the database services are timely detected, documented, and resolved.

Finding 7: Certain SDC security controls related to logical access, vulnerability management, configuration management, user authentication, and logging and monitoring continue to need improvement to ensure the confidentiality, integrity, and availability of SDC and customer entity data and related IT resources.

BACKGROUND

Pursuant to State law,[1] effective July 1, 2020, the Florida Digital Service (FLDS) was created within the Department of Management Services (Department) to provide operational management and oversight of the State Data Center (SDC), among other duties. The State Chief Information Officer administers the FLDS and is appointed by the Department Secretary.[2]

[1] Chapter 2020-161, Laws of Florida.

[2] Section 282.0051(2)(a), Florida Statutes.

According to State law,[3] 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 cybersecurity.
- 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 June 30, 2021, the SDC provided information technology (IT) services to 30 customer entities that contract with the SDC for IT services. The SDC provides its customer entities a variety of IT services and computing environments, including data center facilities and operations, mainframe, network, open systems, storage, cloud, backup and recovery, database, and Windows services, managed applications, and optional customer offerings.

In 2019, the Department contracted with a vendor to prepare a business case that provided a formal recommendation for the best and most appropriate method for the Department to operate the SDC. Completed in March 2020, the business case recommended that a contracted managed service provider (MSP) operate the SDC in full support of the State's cloud-first strategy and efforts to provide quality data processing services, more advanced data analytics, and enhanced interoperability.

On June 30, 2020, the Department posted an Invitation to Negotiate (ITN)[4] for a SDC MSP and respondents were to submit their reply and all required documents by September 14, 2020. On October 12, 2020, the Department began negotiations with three vendors to serve as the SDC MSP and, on March 11, 2021, posted an Intent to Award the MSP contract to one of the three vendors. However, as of January 2022, the Department had not received legislative authorization to execute the agreement for services.

[3] Section 282.201, Florida Statutes.

[4] ITN No. DMS-20/21-031.

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, and Department rules[5] require, for risk assessment purposes, the identification of potential business impacts and likelihoods. State law[6] requires the SDC to develop and implement a disaster recovery plan (DRP), annually conduct a live exercise of the DRP, and maintain performance of the SDC by ensuring proper data backup, data backup recovery, DR, and appropriate security, power, cooling, fire suppression, and capacity. Further, Department rules[7] require that DRPs address shared resource systems, be tested at least annually, and that results of the annual exercise document the plan procedures that were successful and specify any modifications required to improve the plan.

In prior audits of the SDC, most recently in our report No. 2020-149 (Finding 1), we noted that the SDC DRP, annual testing, and processes for customer entities subscribed to SDC DR services needed improvement to ensure that critical SDC operations were recovered and continued in the event of a disaster or other interruption in service. Our follow-up audit procedures found that the SDC completed a live exercise of the SDC DRP on January 22, 2021, and updated the SDC DRP on February 4, 2021. However, our review of the SDC DRP, information included in the Configuration Management Database (CMDB),[8] the service-level agreements (SLAs) with the 13 customer entities (State agencies) who contracted for SDC DR services, and other records found that DR processes continue to need improvement. Specifically, we noted that:

- As part of the BIA process to ensure that all applications critical for DR were identified, the SDC documented within the CMDB the criticality details of each application for DR purposes. From the 123 SDC applications included in the CMDB, we selected 25 applications and examined the related CMDB records, including the records for 22 applications marked urgent criticality, 2 applications marked medium criticality, and 1 application marked low criticality for DR purposes. Our examination found that the CMDB records were not complete for 4 of the urgent criticality applications, the 2 medium criticality applications, and the low criticality application. Specifically, CMDB records for these 7 applications did not evidence that the BIA performed in November 2020 included an updated criticality review and one or more fields on the CMDB criticality details page were not updated. In response to our audit inquiry, SDC management indicated that application owners were responsible for updating the CMDB records and, due to oversight, the CMDB records were not updated to evidence review for the BIA.
- While the SDC DRP indicated that the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) thresholds were identified in Section 2 of the DRP, no such information was

[5] Department Rule 60GG-2.002(4)(b)4., Florida Administrative Code.

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

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

[8] The CMDB supports SDC IT service management processes such as service request management, incident management, and change/release management. The CMDB is to include assets in inventory such as servers, applications, clusters, databases, and network devices, as well as the relationships between services and configuration items.

included. According to SDC management, the RPO and RTO thresholds were inadvertently omitted when the DRP was updated.

- For 1 application marked in the CMDB as having urgent criticality and required for DR, the SDC DRP, including the incorporated DR testing runbook, did not include step-by-step instructions for recoverability and the related systems necessary to recover the application. In response to our audit inquiry, SDC management indicated that application infrastructure issues required resolution and these efforts were delayed due to ongoing technical issues with the application, ongoing procurement of related infrastructure, and contract negotiations with the MSP.
- As of January 12, 2022, 2 applications had not been subject to DR testing although the applications were identified as critical applications in DRP testing documentation for the 2020-21 fiscal year. According to SDC management, testing for these applications was delayed due to ongoing technical issues with the applications and the MSP contract negotiations.
- Necessary updates to CMDB information for 3 of the 22 applications marked urgent criticality in the CMDB were not made following the DR exercises in December 2020. Specifically, as of August 4, 2021, the infrastructure supporting the applications was either not included in the CMDB records or was marked as not included for DR. According to SDC management, the information was omitted or not marked for DR due to application owner oversight.
- While DR testing runbook documentation was updated for the December 2020 DR exercises, additional testing in January 2021 to complete the live exercises for the 2020-21 fiscal year were not recorded in the runbook documentation. In response to our audit inquiry, SDC management indicated that the January 2021 live exercises were not included in the runbook documentation because the information was overwritten or not updated due to an oversight.
- Section 4 of the DRP stated that customer entities subscribed to the SDC DR offering were to be prioritized first for recovery, and that subscribers who supported critical functions, including public health and safety services, were to be prioritized first of the subscribed customer entities. However, our audit found that a specific recovery order had not been established for the 13 subscribed customer entities, their applications, or systems. According to SDC management, additional guidance was necessary from FLDS management and those responsible for governance on the recovery order in the event of a disaster affecting multiple customer entities.
- In May 2020, a limited full-scale exercise for the 13 customer entities subscribed to DR services was performed to ensure that the assets (systems and applications) for each customer entity were operational in the event of a disaster at the DR site. However, a complete full-scale exercise that included failover of customer systems and applications from the SDC to the DR site did not occur because scheduling conflicts with the customer entities prevented a simultaneous test.

For the 13 customer entities subscribed to DR services, we also examined, as of July 22, 2021, the most recent DR exercise results reports and supporting documentation. Our examination disclosed that, for 4 customer entities, a DR exercise was not completed for the 2020-21 fiscal year. In response to our audit inquiry, SDC management indicated that the exercise was not completed for 3 customer entities due to the lack of a circuit connecting the mainframe service provider and the offsite DR location. For the other customer, dependencies associated with an application experiencing technical issues that the SDC was unable to resolve resulted in the postponement of the DR exercise.

Conducting a BIA that includes a review of the criticality of all SDC applications for DR purposes, defining RPO and RTO thresholds, providing step-by-step instructions for the recovery of each critical application in the DRP, and conducting and documenting live DR exercises for all critical applications decreases the risk that critical SDC applications will not be recovered in a timely and orderly manner in the event of a disaster or other interruption in service. Full-scale testing to prepare for an outage event affecting all

customer entities, completing an annual DR exercise for all DR customers, and establishing a recovery order for customer entities decreases the risk that critical customer entity applications, systems, and related infrastructure will not be recovered timely and orderly 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 again recommend that Department management improve disaster recovery processes and related documentation. Specifically, we recommend that Department management:

- **Conduct a BIA that documents the assessment of the criticality of all SDC applications for DR purposes.**
- **Update the SDC DRP to include RPO and RTO thresholds.**
- **Develop step-by-step recovery instructions for, and conduct testing of, all applications included in the DRP and ensure that CMDB records are updated, as necessary, for all critical SDC-managed applications in the DRP.**
- **Ensure documentation of live DR exercises is maintained.**
- **Establish a recovery order for subscribed customer entities in the event of a disaster affecting multiple customers and ensure that full-scale testing is performed to verify that all applications, systems, and related infrastructure can be timely restored.**
- **Ensure DR exercises are conducted annually for all subscribed customer entities.**

Finding 2: Continuity of Operations Planning

Continuity of operations planning is 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 plan and annually conduct a live exercise of the plan. State law[10] also requires that a disaster preparedness plan (i.e., a Continuity of Operations Plan, or 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 maintained a COOP[11] with references to the SDC DRP for certain information. Our evaluation of the COOP and related documentation found that:

- Although the COOP referenced the DRP which listed the servers containing databases supporting critical SDC applications, the specific database names were not included in the COOP and the database list included in the DRP documentation only included one specific database name.
- The COOP included neither delegations of authority nor lines of succession.

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

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

[11] FLDS Continuity of Operations Plan DST-BCOS-MS-001.

In response to our audit inquiry, SDC management indicated that various critical databases had been identified and tested during DR exercises in December 2020 and January 2021; however, the list of the included databases was not maintained in the DRP documentation due to a management decision. Additionally, SDC management indicated that executive and management changes needed to be finalized prior to defining delegations of authority and lines of succession.

Identification in the SDC COOP or related documentation of vital databases, delegations of authority, and lines of succession would comply with State law and promote the continuity of critical State functions and the availability of related information in the event of a disaster or other interruption of service. A similar finding was noted in prior audits of the SDC, most recently in our report No. 2020-149 (Finding 2).

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

Finding 3: Backup Tape Reconciliations

Department rules[12] require the mirroring, or creation of regular backups or current copies, of data and software essential to the continued operation of critical agency functions with storage at an off-site location. To facilitate the recovery of data from backup tape media, effective backup controls include policies, procedures, and processes to ensure that accurate records of the location and status of backup data are maintained. Such controls facilitate the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

Our audit procedures disclosed that SDC reconciliation controls for backup tape media were insufficient. Specifically:

- While SDC procedures[13] required a semiannual reconciliation of the backup system tape records to the records in the tape tracking system, a reconciliation was not performed during the 2020-21 fiscal year and SDC management was unable to determine the date of the last reconciliation. According to SDC management, the SDC Backup and Recovery Section had insufficient personnel to perform the required reconciliations.
- Absent a reconciliation by SDC personnel, we compared the active tapes listed on the backup system reports to the active tapes listed on reports from the tape tracking system and found that 552 tapes listed on the tape tracking system reports were not included on the backup system reports. We also noted 8 tapes listed on the backup system reports that were not listed on the tape tracking system reports. In response to our audit inquiry, SDC management acknowledged that 380 tapes listed on the tape tracking system reports were missing from the backup system reports because the backup system reports did not accurately reflect the active tapes. SDC management further indicated that the other 172 tapes were missing from the backup system reports because reporting from the legacy system that created the tapes was no longer available; however, the tapes were still being maintained at the SDC and therefore were active tapes. SDC management indicated that the 8 tapes missing from the tape tracking system reports were data backups created and provided directly to a State agency customer upon request; however, no records documenting the tape numbers provided to the State agency customer were maintained.

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

[13] FLDS Tape Management and Reconciliation Procedure DST-BIOS-P-209.

Complete and timely periodic reconciliations of backup tape records 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 of production data. A similar finding was noted in prior audits of the SDC, most recently in our report No. 2020-149 (Finding 4).

Recommendation: We again recommend that Department management ensure that semiannual reconciliations of backup system tape records to tape tracking system records are performed and documented in accordance with Department procedures.

Finding 4: Periodic Review of Access Privileges

Department rules[14] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of user and service accounts with access to data and IT resources help protect the confidentiality, integrity, and availability of data and IT resources by ensuring that only authorized users have access and that the access privileges assigned to user and service accounts remain appropriate and necessary. An effective periodic review consists of identifying the current access privileges of system users and services and evaluating the assigned access privileges to ensure that they align with user job responsibilities or service account requirements.

In our report No. 2020-149 (Finding 6), we noted that SDC processes for performing and documenting periodic access reviews needed improvement. As part of our audit and evaluation of SDC access controls, we noted that SDC periodic access privilege review processes did not adequately ensure that assigned access privileges remained appropriate. Specifically:

- In response to our request for documentation of periodic reviews performed for Windows server local administrative accounts and Active Directory administrative accounts, SDC management indicated that, in accordance with the SDC *Active Directory Account Audit Procedure*, periodic reviews of administrative accounts were initiated using a scheduled task that ran a script biweekly in all SDC-managed domains. The script generated a report of administrative accounts for each domain and automatically converted the reports to service requests requiring SDC personnel review. Our examination of the reports generated on June 14, 2021, and June 28, 2021, found that the reports did not include all administrative accounts for the respective domains. Instead, the script only reported the *Enterprise*, *Schema*, and *Domain Admins* security groups for Active Directory and did not include in the reports the *Administrators* security group. Additionally, reports were not generated, nor was access reviewed, for Windows server local administrative accounts. In response to our audit inquiry, SDC management indicated that the script was created in 2017 and, although modified in 2018, neither the *Administrators* security group nor the Windows server local administrative accounts were added to the script.
- For Oracle database access, SDC management only reviewed the access of Database Section personnel on an annual basis and the reviews were limited to verifying the authorizations for individually assigned accounts in the service management system. Additionally, the reviews were not conducted from a system-generated listing of all active administrative Oracle database accounts and, as a result, administrative accounts for the SDC-managed Oracle databases could be omitted from review. Although SDC management indicated in response to our audit inquiry that the existing reviews were sufficient, the reviews excluded access assigned to shared administrative accounts and accounts assigned to individuals outside of the Database Section,

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

such as SDC personnel, customer entities, and historical accounts from prior data center administrations.

- For open systems access, SDC management annually reviewed administrative-level access to the open systems servers by verifying the access authorizations in the service management system for Open Systems Section personnel. However, the reviews were not conducted using a system-generated list of the administrative-level accounts for each server and, as a result, accounts on the open systems servers could be omitted from review. In response to our audit inquiry, SDC management indicated that the reviews were sufficient because all Open Systems personnel with root shell access had the same access privileges for all open systems servers, and that periodic reviews on a server-by-server basis would yield the same results as the existing reviews from the service management system. Notwithstanding, the reviews performed excluded access assigned to individuals outside the Open Systems Section, such as other SDC personnel, SDC customer entities, and historical accounts from prior data center administrations.

Absent comprehensive reviews of logical access privileges using system-generated lists, management's assurance that access privileges were properly authorized and remain appropriate is limited.

Recommendation: We again recommend that Department management ensure that comprehensive and documented periodic reviews of logical access privileges are conducted using system-generated lists of all user and service accounts.

Finding 5: Backup Controls

State law[15] requires the SDC to maintain performance of the SDC by ensuring proper data backup and data backup recovery. Further, the SDC's SLAs[16] with their customer entities specified that the Data Protection Service was to provide scheduled backups of customer entity data contained within the SDC and on supported, managed, or co-located operating systems within the designated backup window. The Data Protection Service was also to provide data protection reporting for customer visibility. Department rules[17] require State agencies to ensure that backups of information are conducted, maintained, and tested.

Our review of backup procedures performed as of April 14, 2021, for 40 of the 2,304 production Windows, Linux, or Solaris physical and virtual servers managed by the SDC as of March 24, 2021, found that SDC backup controls need improvement. As similarly noted in prior audits of the SDC, most recently in our report No. 2020-149 (Finding 7), we found that for 7 servers the SDC had not successfully completed the required daily (incremental) or weekly (full) backups and, for another 5 servers, backup records were incomplete. Specifically for:

- 3 virtual servers and 1 physical server, the SDC was unable to provide evidence of the two most recent daily backups or the most recent weekly backup. For 2 of the 3 virtual servers, SDC management acknowledged that, due to the operating system used for the servers, evidence of backup was not available. In addition, although requested, the SDC was unable to provide evidence of the backup of the related physical host servers. For the other virtual server and the physical server, SDC management indicated that the servers had been decommissioned; however, our review of SDC IT service management system records showed that, while the SDC

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

[16] SDC FY 2020-2021 Service Catalog, Attachment A, Data Protection Service.

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

planned to decommission the servers, the physical server was still active as of May 19, 2021, and the virtual server was still active as of June 16, 2021.

- 1 virtual and 1 physical server, the most recent backup on April 12, 2021, failed and, as of April 14, 2021, a successful backup had not been performed. In response to our audit inquiry, SDC management indicated that the backups failed due to an internal processing error. Subsequently, the issue was resolved and backups of the 2 servers were completed on April 16, 2021.
- 1 physical server, the weekly full backup for April 11, 2021, was not performed. According to SDC management, a prior daily backup job for the server on April 10, 2021, ran for 2 days, preventing the weekly full backup.
- 5 physical servers, the SDC was unable to provide backup reports that showed the type of backup performed (i.e., incremental or full) and whether the backup job completed successfully. According to SDC management, the reporting software was not functioning properly and, as a result, backup reports were unavailable.

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

Recommendation: We again recommend that Department management ensure that all required server backups are timely and successfully performed, and that evidence of the backups, including system-generated reports, is maintained.

Finding 6: Performance Metrics

Effective IT performance management requires a monitoring process that includes defining relevant performance metrics and the systematic and timely reporting of performance in relation to the performance metrics. Pursuant to State law,[18] the SDC is to establish in SLAs with customer entities the metrics and processes by which the business standards for each service provided to the customer entities are to be objectively measured and reported. The *SDC Overview of Oracle Service Standards and Policies* required all Oracle database host servers to be monitored 24 hours a day, 7 days a week, by the Oracle monitoring system (the primary monitoring system) and the SLAs required Oracle database uptime a minimum of 99.5 percent of the monthly scheduled availability for each respective database.

Our audit included an evaluation of the SDC's achievement of targeted performance metrics for uptime for the customer production Oracle databases. Our evaluation of the performance metrics and related uptime statistics for 14 of the 63 stand-alone production Oracle databases during the period July 2020 through April 2021 found that the performance metrics and related uptime statistics for 10 databases were not retained in the Oracle monitoring system. Specifically, monthly data was missing for 2 databases for 1 month, 5 databases for 2 months, and 3 databases for 3 months. As a result, we were unable to determine for the 10 databases whether the monthly uptime performance metric was met for those months. In response to our audit inquiry, SDC management indicated that the data loss occurred during an upgrade of the monitoring system and they were unaware that they needed to save the performance metrics and related uptime statistics prior to the upgrade.

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

Our examination of the monthly performance metrics and related uptime statistics available for the 14 selected databases found that the SDC did not meet the monthly performance metric of 99.5 percent for 2 of the customer entity databases. Specifically, for 1 customer database, the uptime for December 2020 was 87.4 percent. For the other customer database, the uptime was less than 99.5 percent for 4 consecutive months (September 2020 through December 2020), ranging from zero to 71.4 percent (an average of 27.6 percent). In response to our audit inquiry, SDC management indicated that the downtime for the first database resulted from a failed software patch and that the database was restored when the database server was repaired a week later. For the other database, SDC management indicated that network connectivity issues impacted the database uptime. SDC management also noted that data from a secondary monitoring system showed that the database was up during part of the period and that they believed the downtime recorded by the primary monitoring system was overstated because the primary monitoring system may not have been enabled by the database administrator after maintenance on the database was performed.

Effective database performance monitoring is essential to the timely detection and resolution of critical incidents involving database services. Additionally, without complete records, the SDC cannot demonstrate the accuracy of reported uptime statistics or compliance with SLA performance metrics. Similar findings were noted in prior audits of the SDC, most recently in our report No. 2020-149 (Finding 9).

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

Finding 7: Security Controls – Logical Access, Vulnerability Management, Configuration Management, User Authentication, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain SDC security controls related to logical access, vulnerability management, configuration management, user authentication, and logging and monitoring need improvement. 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, vulnerability management, configuration management, user authentication, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of SDC and customer entity data and related IT resources may be compromised. Similar findings were communicated to Department management in connection with prior audits, most recently in connection with our report No. 2020-149.

Recommendation: We again recommend that Department management improve certain security controls related to logical access, vulnerability management, configuration management, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of SDC and 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 findings included in our report No. 2020-149.

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 information technology (IT) operational audit from March 2021 through November 2021 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 significant IT controls applicable to State Data Center (SDC) operations during the period July 2020 through June 2021 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2020-149.
- 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 that were significant to our audit objectives; 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 and evaluating the IT systems and related significant 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:

- Reviewed applicable laws, rules, Department of Management Services (Department), Florida Digital Service, and SDC policies and procedures, and other guidelines and interviewed Department personnel to obtain an understanding of the SDC organizational structure, statutory requirements, and operational processes.
- Interviewed Department and SDC personnel and examined SDC records to obtain an understanding of the SDC IT infrastructure and architecture, including hardware, software, and operating systems for the various server platforms, network components, and database management systems.
- Interviewed SDC personnel to obtain an understanding of the SDC services offered, customer entities served, and the division of responsibilities between the SDC and customer entities.
- Evaluated SDC compliance with requirements defined in customer service-level agreements for performance uptime monitoring for the Oracle databases and the interconnected network infrastructure. Specifically, we examined:
    - The monthly performance metrics and related uptime statistics for 14 of the 63 stand-alone production Oracle databases during the period July 2020 through April 2021 to determine whether the SDC met the monthly uptime performance metric and SDC records accurately reflected database uptime performance.
    - The monthly network service performance metrics and related uptime statistics for 6 of the 30 SDC customer entities during the period February 2021 through April 2021 to determine whether the SDC met the monthly uptime performance metric and SDC records accurately reflected network uptime performance.
- Evaluated the adequacy of IT asset management processes for IT inventory tracking and reconciliation of SDC-managed physical assets in the data center cabinets, SDC processes for ensuring the accuracy of the hardware and software configuration records in the Configuration Management Database (CMDB), and the performance of ongoing CMDB audits by SDC personnel.
- Evaluated the adequacy of the SDC continuity of operations plan and determined whether the SDC had conducted a live exercise of the plan in accordance with Section 282.201(1)(c), Florida Statutes.
- Evaluated the adequacy of the SDC disaster recovery plan, including whether the SDC had:
    - Conducted a live exercise of the plan in accordance with Section 282.201(1)(c), Florida Statutes, and remediated identified issues and modified the plan based on exercise results.

- Conducted a business impact analysis to identify all SDC critical applications for recovery.
- Evaluated disaster recovery processes for customer entities subscribed to SDC disaster recovery services.

- Evaluated the adequacy of the policies, procedures, and processes for the management and monitoring of software licensing at the SDC.
- Evaluated SDC backup policies, procedures, and processes, including the performance of daily and weekly server backups, backup media recoverability testing, and backup tape reconciliations, storage, and destruction processes. Specifically, we:
  - Examined the most recent daily and weekly backup reports as of April 14, 2021, for 40 of the 2,304 Windows, Linux, or Solaris production servers as of March 24, 2021, to determine whether the SDC performed required backups.
  - Evaluated whether the SDC performed annual recoverability testing of selected backup media.
  - Evaluated whether the SDC conducted periodic reconciliations of backup tape records to ensure that backup tape media location records remained accurate and complete.
  - Evaluated whether SDC backup tape media was securely stored off-site.
  - Examined tape destruction records for 45 of the 18,715 tape records with a destroyed status in the tape tracking system as of March 25, 2021, to determine whether the SDC maintained accurate records of approval and destruction.
  - Evaluated administrative access privileges for the tape tracking system to determine whether account access privileges were appropriately assigned.
- Examined SDC tape encryption procedures and evaluated the adequacy of the procedures and related tape encryption processes, including the performance of monthly encryption audits.
- Evaluated the effectiveness of SDC policies, procedures, and processes for vulnerability management, including scanning, analysis, and remediation of reported vulnerabilities for the SDC Windows, open systems, mainframe, and network environments.
- Evaluated the adequacy of the incident response and remediation of specific known vulnerabilities.
- Evaluated the adequacy of SDC policies and processes for authorizing, removing, periodically reviewing, logging, and monitoring physical access to the SDC facility and Sadowski Building, including evaluating the 29 key cards with unlimited access to the SDC facility as of May 12, 2021.
- Evaluated the design, authorization, administration, and periodic review procedures for logical access privileges to SDC IT resources and customer entity data. Specifically, we evaluated:
  - The appropriateness of access privileges for the 22 active Resource Access Control Facility (RACF) administrative accounts with one or more selected elevated access authorities assigned across four mainframe logical partitions (LPARs) as of June 29, 2021.
  - The appropriateness of access privileges for 15 of the 103 active RACF administrative accounts with one or more selected elevated access authorities for another mainframe LPAR as of May 6, 2021.
  - The appropriateness of access privileges for the 17 active CA Top Secret administrative accounts with unlimited scope assigned across two mainframe LPARs as of May 11, 2021.
  - The appropriateness of access privileges for the 83 active Access Control Facility 2 (ACF2) administrative-level accounts with a selected elevated access privilege for a mainframe LPAR as of May 13, 2021.

- The appropriateness of administrative-level access for the three network domains used for SDC services and operations as of April 12, 2021, and May 5, 2021.
- For 40 of the 1,663 Windows production servers as of March 24, 2021, the appropriateness of access privileges for the 318 accounts with administrative-level access privileges to their respective Windows servers as of April 2, 2021.
- The appropriateness of administrative-level access privileges for 26 accounts on 17 of the 209 Red Hat Enterprise Linux production servers as of May 10, 2021.
- The appropriateness of access for the 11 individuals with access to the open systems shared administrative-level accounts stored in the password vault as of August 10, 2021.
- The appropriateness of administrative-level access privileges on 6 of the 20 production Oracle database clusters as of June 15, 2021, and July 12, 2021.
- The adequacy of periodic review procedures for administrative-level logical access privileges for the Windows, network, open systems, and Oracle database environments.

- Evaluated the adequacy of SDC IT infrastructure user identification and authentication controls. Specifically, we examined the:
  - RACF user authentication controls for six mainframe LPARs as of May 14, 2021.
  - ACF2 user authentication controls for one mainframe LPAR as of May 14, 2021.
  - CA Top Secret user authentication controls for two mainframe LPARs as of May 14, 2021.
  - User authentication controls for the two SDC network domains as of April 12, 2021, and one Department domain as of May 5, 2021.
  - User authentication controls for 28 of the 220 Red Hat Enterprise Linux production servers as of May 10, 2021.
  - User authentication controls for 6 of the 20 Oracle production cluster databases as of June 15, 2021, and July 12, 2021.
  - User authentication controls for ten selected high-risk network devices as of March 25, 2021, and March 30, 2021.
- Evaluated the effectiveness of SDC configuration management policies, procedures, and processes for servers and high-risk network devices. Specifically, we evaluated:
  - Ten high-risk network devices to determine whether, as of March 25, 2021, the SDC timely installed vendor-supplied patches.
  - 28 of the 198 SDC-managed Red Hat Enterprise Linux production lifecycle servers as of March 24, 2021, to determine whether, as of April 7, 2021, the operating system software was supported and anti-malware software was up-to-date.
  - 40 of the 1,511 vendor-supported Windows production servers as of March 24, 2021, to determine whether, as of April 16, 2021, the SDC timely installed vendor-supplied patches.
  - 41 of the 1,483 vendor-supported Windows production servers as of July 20, 2021, to determine whether, as of July 28, 2021, the SDC had timely installed a vendor-supplied patch addressing a critical vulnerability.
- Evaluated the effectiveness of SDC logging and monitoring controls.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.

- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

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

Sherrill F. Norman, CPA
Auditor General

EXHIBIT A

LIST OF STATE DATA CENTER CUSTOMER ENTITIES

AS OF JUNE 30, 2021

	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 Corrections
7	Department of Economic Opportunity
8	Department of Education
9	Department of Elder Affairs
10	Division of Emergency Management
11	Department of Environmental Protection
12	Department of Health
13	Department of Highway Safety and Motor Vehicles
14	Department of Juvenile Justice
15	Department of the Lottery
16	Department of Management Services
17	Department of Military Affairs
18	Department of Revenue
19	Department of State
20	Department of Transportation
21	Department of Veterans' Affairs
22	Executive Office of the Governor
23	Florida Fish and Wildlife Conservation Commission
24	Greater Orlando Aviation Authority
25	Justice Administrative Commission
26	Miami-Dade Expressway Authority
27	Northwest Florida Water Management District
28	Public Employee Relations Commission
29	Public Service Commission
30	Santa Rosa County

Source: Brandon Tedder, Cloud Architect, Office of Infrastructure and Modernization, Florida Digital Service.

MANAGEMENT'S RESPONSE

Department of MANAGEMENT SERVICES
We serve those who serve Florida

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

Ron DeSantis, Governor
J. Todd Inman, Secretary

March 28, 2022

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, enclosed 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 findings.

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

Sincerely,

J. Todd Inman
Secretary

JTI/tam

Enclosure

cc: James Grant, State Chief Information Officer
Sarah B. Hall, Inspector General

Responses to Preliminary and Tentative Findings

Finding 1: Disaster Recovery Planning
The SDC's disaster recovery plan [DRP] and related business impact analysis [BIA], annual testing, and recovery processes for customer entities subscribed to [State Data Center] SDC disaster recovery services continue to need improvement to ensure that critical SDC and customer 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 again recommend that Department management improve disaster recovery processes and related documentation. Specifically, we recommend that Department management: • Conduct a BIA that documents the assessment of the criticality of all SDC applications for DR purposes. • Update the SDC DRP to include [recovery point objective] RPO and [recovery time objective] RTO thresholds. • Develop step-by-step recovery instructions for, and conduct testing of, all applications included in the DRP and ensure that [configuration management database] CMDB records are updated, as necessary, for all critical SDC-managed applications in the DRP. • Ensure documentation of live DR exercises is maintained. • Establish a recovery order for subscribed customer entities in the event of a disaster affecting multiple customers and ensure that full-scale testing is performed to verify that all applications, systems, and related infrastructure can be timely restored. • Ensure DR exercises are conducted annually for all subscribed customer entities.
State Agency Response and Corrective Action Plan: • The SDC performed a BIA and will work to improve the process and documentation. • Processes to update the CMDB will be improved to better facilitate documentation related to the applications in the DRP including RPO and RTO thresholds. • A full-scale system recovery exercise was performed, but due to scheduling constraints customer application testing was not performed. However, the SDC will work with customers to schedule a full-scale exercise recovery test. • Recovery priority determinations for all State systems are likely beyond the purview of the SDC. The SDC can perform the recovery, however it does not make decisions on the relative priority for State systems. • The SDC continues to offer annual testing to all subscribed customers; and • The SDC will explore options to improve the ability of customers to participate in annual DR exercises.
Projected Completion Date: N/A – Pending Legislative action could change responsible parties/completion timeline.

Finding 2: Continuity of Operations Planning
As similarly noted in prior audits, most recently in our report No. 2020-149, SDC continuity of operations plan [COOP] documentation did not include all essential information specified in State law.
Recommendation:
To promote the continued operations of the SDC, we again recommend that Department management include in the SDC COOP, or incorporate by reference, all essential information specified in State law.
State Agency Response and Corrective Action Plan:
The SDC has the information necessary to perform COOP operations. However, COOP staff will work with the DR team to make improvements to references and update the SDC COOP with identified essential personnel.
Projected Completion Date: 7/1/2022

Finding 3: Backup Tape Reconciliations
SDC processes for reconciling backup tapes were insufficient to ensure that all backup tapes were accounted for and backup records were accurate.
Recommendation:
We again recommend that Department management ensure that semiannual reconciliations of backup system tape records to tape tracking system records are performed and documented in accordance with Department procedures.
State Agency Response and Corrective Action Plan:
Subsequently to the Auditor General's fieldwork, the SDC completed a reconciliation on February 18, 2022.
Projected Completion Date: N/A – Already completed.

Finding 4: Periodic Review of Access Privileges
As similarly noted in our report No. 2020-149, SDC processes for performing and documenting periodic access reviews for the network, Windows server, open systems, and Oracle database environments did not adequately ensure that assigned access privileges remained appropriate.
Recommendation:
We again recommend that Department management ensure that comprehensive and documented periodic reviews of logical access privileges are conducted using system-generated lists of all user and service accounts.
State Agency Response and Corrective Action Plan:
The SDC will continue to improve and enhance the process and scope related to review of access privileges.
Projected Completion Date: N/A – Pending Legislative action could change responsible parties/completion timeline.

Finding 5: Backup Controls
SDC backup controls continue to need improvement to ensure that backups for all IT resources requiring backup are appropriately performed and documented.
Recommendation: We again recommend that Department management ensure that all required server backups are timely and successfully performed, and that evidence of the backups, including system-generated reports, is maintained.
State Agency Response and Corrective Action Plan: We agree that timely, complete, and successful backups are important. We will continue to evaluate the backup processes for improvement to ensure that backups are timely completed, and system-generated reporting of the backups is maintained.
Projected Completion Date: **N/A – Pending Legislative action could change responsible parties/completion timeline..**

Finding 6: Performance Metrics
The SDC's monitoring and reporting of the performance metrics for database services provided to customer entities continue to need improvement to ensure that critical incidents affecting the database services are timely detected, documented, and resolved.
Recommendation: We again recommend that Department management ensure that SDC database performance uptime metrics included in the SLAs are met and appropriate documentation for performance metrics and related uptime statistics is maintained.
State Agency Response and Corrective Action Plan: The SDC will continue to investigate additional process improvements to increase data quality. The SDC continues to collect metrics to meet SLA performance metrics.
Projected Completion Date: **N/A – Pending Legislative action could change responsible parties/completion timeline.**

Finding 7: Security Controls – Logical Access, Vulnerability Management, Configuration Management, User Authentication, and Logging and Monitoring
Certain SDC security controls related to logical access, vulnerability management, configuration management, user authentication, and logging and monitoring continue to need improvement to ensure the confidentiality, integrity, and availability of SDC and customer entity data and related IT resources.
Recommendation: We again recommend that Department management improve certain security controls related to logical access, vulnerability management, configuration management, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of SDC and customer entity data and related IT resources.

State Agency Response and Corrective Action Plan:
The SDC will continue to evaluate and improve security controls to ensure the confidentiality, integrity and availability of data and IT resources.
Projected Completion Date: N/A – Ongoing effort. Pending legislative action could change responsible parties and completion timelines.