



An Audit Report on

The Department of Information Resources' Data Center Services Contracts

- The Department complied with applicable requirements for contract monitoring.
- User access controls for the Department's contract management system should be updated to ensure appropriate access.
- The Department did not fully implement prior audit recommendations addressing asset management and board training for contracting.

Lisa R. Collier, CPA, CFE, CIDA
State Auditor

The Department of Information Resources (Department) complied with applicable contract monitoring requirements for the two Data Center Services contracts selected for review: Texas Private Cloud, Facilities and Computing Services; and Technology Solution Services. However, the Department should strengthen its controls over user access.

Although the Department implemented some processes based on recommendations from prior audits, it did not fully implement recommendations related to training in contracting for board members, tracking and securing assets, or documenting media sanitization for all asset disposals and transfers.

- [Background](#) | p. 4
- [Audit Objective](#) | p. 17

This audit was conducted in accordance with Texas Government Code, Sections 321.013 and 321.0132.

MEDIUM

PERFORMANCE MONITORING

The Department had adequate processes and controls for monitoring performance. However, the Department should strengthen user access controls for its contract management system.

[Chapter 1-A | p. 8](#)

LOW

FISCAL MONITORING

The Department had adequate processes and controls for monitoring payments and invoices.

[Chapter 1-B | p. 11](#)

NOT RATED

PRIOR RECOMMENDATIONS

The Department substantially implemented one recommendation from a prior audit; corrective action was incomplete or ongoing for two other recommendations.

[Chapter 2 | p. 13](#)

For more information about this audit, contact Audit Manager Michael Simon or State Auditor Lisa Collier at 512-936-9500.

July 2023 | Report No. 23-038

Summary of Management's Response

Auditors made recommendations to address the issues identified during this audit, provided at the end of Chapter 1-A in this report. The Department agreed with the recommendations.

Ratings Definitions

Auditors used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings in relation to the audit objective.

PRIORITY: Issues identified present risks or effects that if not addressed could *critically affect* the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

HIGH: Issues identified present risks or effects that if not addressed could *substantially affect* the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

MEDIUM: Issues identified present risks or effects that if not addressed could *moderately affect* the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

LOW: The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks *or* effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

For more on methodology for issue ratings, see [Report Ratings](#) in Appendix 1.

Background Information

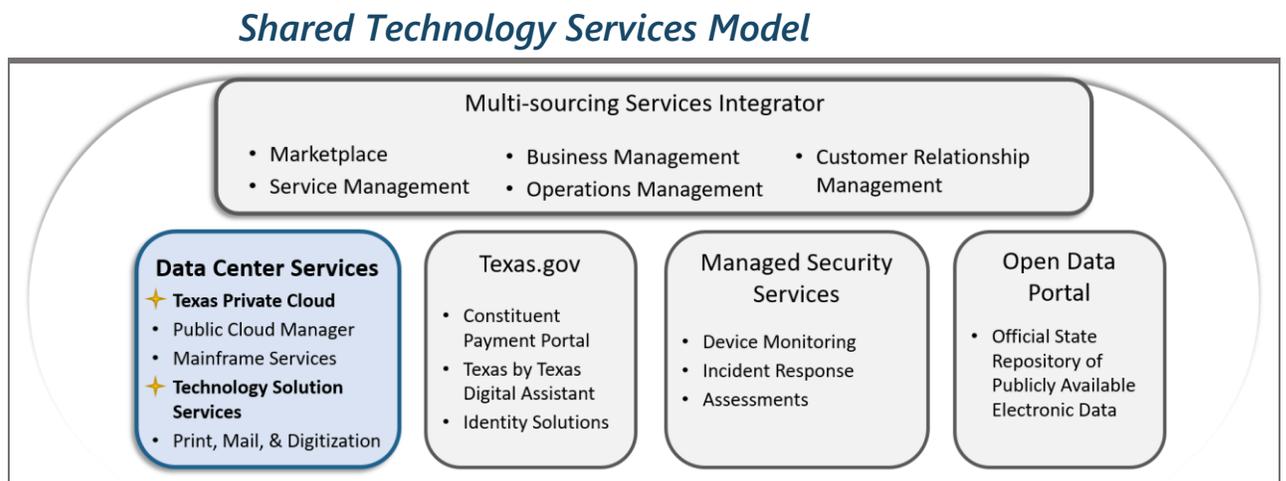
The Legislature created the Department of Information Resources (Department) in 1989 through Texas Government Code, Section 2054 (the Information Resources Management Act). The Department administers information security, information technology, and telecommunications services for state and local government entities.

Shared Technology Services and Data Center Services

Shared Technology Services. The Department established its Shared Technology Services model in accordance with Texas Government Code, Section 2054.378. The statute authorizes the Department to operate or contract to operate statewide technology centers to provide services relating to (1) information resources technology and (2) the deployment, development, and maintenance of software applications.

The model encompasses four programs (see Figure 1). In addition, it includes a contract for a multi-sourcing services integrator (MSI) to oversee contractors that provide services within the programs. These contractors are known as service component providers.

Figure 1



Source: Information provided by the Department.

Data Center Services (DCS). This audit focused on two contracts in the DCS program: (1) Texas Private Cloud, Facilities and Computing Services, and (2)

Technology Solution Services. The program allows the Department's customers, which are state and local government entities, to outsource management of technology infrastructure services. The customer base included 90 entities, as of July 2022, according to the Department.

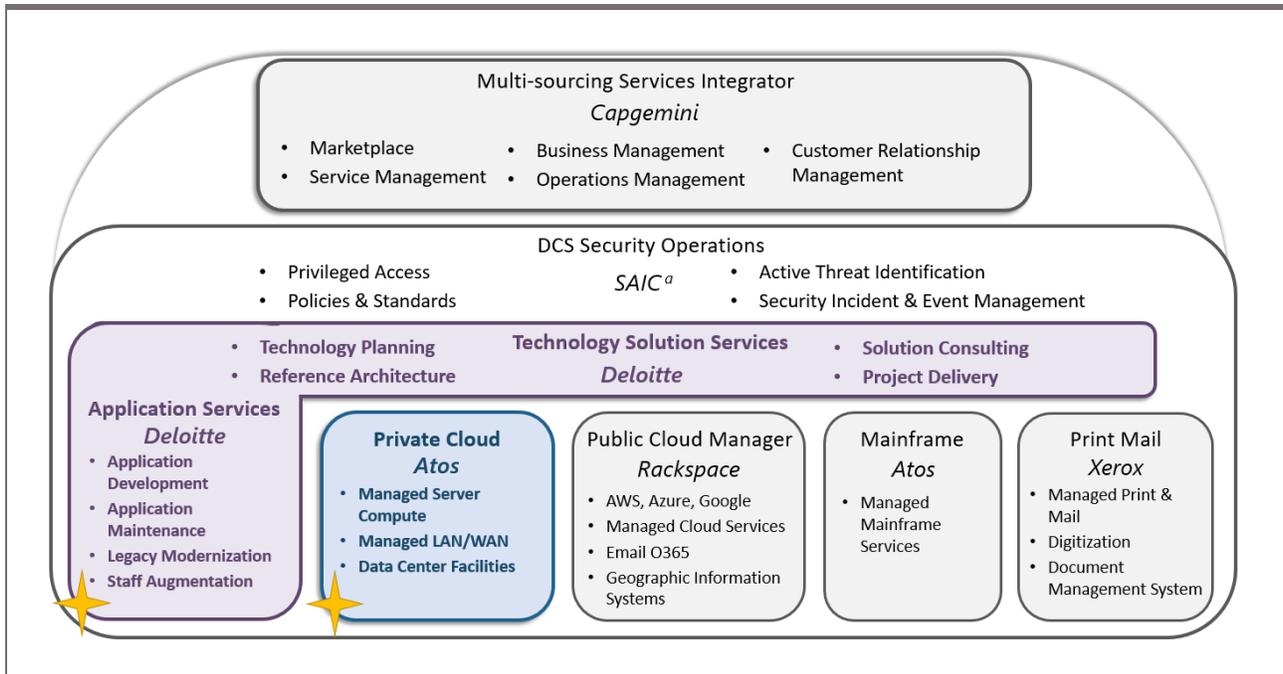
The Department's next-generation DCS model, which was implemented on September 1, 2020, uses multiple cross-functional contracts to help develop and maintain statewide technology centers, information resources, and software applications. The contracts include:

- **MSI.** Capgemini America Inc. provides systems, processes, and service delivery oversight to support a common delivery model for services by the component providers and to assist the Department in monitoring them.
- **DCS Security Operations.** Science Application International Corporation (SAIC) monitors security, manages security threats and events, and controls service component providers' access to customer systems.
- **Technology Solution Services.** Deloitte Consulting LLP provides customers with access to technical architects, project management, and help in modernizing systems; in addition, it offers application development, maintenance, and staff augmentation services. Services may be provided only for applications on DCS infrastructure.
- **Infrastructure.** Atos Government IT Outsourcing Services LLC (Atos) maintains the state data centers and management of mainframe services used by the DCS program. Rackspace US Inc. provides public cloud services.

See Figure 2 on the next page for an overview of the model with additional details on services and contractors.

Figure 2

Data Center Services Model



^a Science Application International Corporation.

Source: Information provided by the Department.

Owner-operator Governance Model

The **Owner-operator Governance Model** requires the Department and customers to participate in governance of contracts, including DCS program decisions and resolution of customer issues. Customers agree to work with service component providers to resolve operational issues and to participate in governance committees to address program-level matters.

Inter-agency and Inter-local Contracts. Customers commit to complying with this model in an inter-agency contract or inter-local contract with the Department. The contract must be completed before services from the shared technology services contracts can be used.

Customer Responsibilities. Customers agree to support the services and standards in the contracts, by adhering to established technology standards

and collaborating with service component providers to support changes to systems. In addition, customers are responsible for reporting progress to the State's quality assurance team for any applications purchased through the program that cost more than \$10 million, as required by Texas Government Code, Section 2054.159(f).

Contracts Selected for Audit

This audit focused on the Department's monitoring of the following contracts:

- **Texas Private Cloud, Facilities and Computing Services** – Atos maintains two geographically separated, consolidated data centers providing technology infrastructure computing and storage. The Department paid \$234,245,857 to the contractor from September 1, 2020, through December 31, 2022.
- **Technology Solution Services** – Deloitte provides customers with technical strategy management, solution design, and project delivery for DCS infrastructure. The contractor also provides managed application services and staff augmentation services for applications hosted in the program's public and private clouds. The Department paid \$192,859,423 to the contractor from September 1, 2020, through December 31, 2022.

The DCS program uses controls at the customer, MSI, and service component provider levels, along with the Department's controls, to fulfill the Department's and the contractors' commitments.

This audit did not involve any work with customers or with other service component providers. It did not include tests to determine whether contractors complied with significant terms of the two selected contracts, other than the contractors' participation in monitoring processes established in the contracts and their compliance with the Department's policies and procedures. Please see Appendix 1 for more details about the scope of the audit.



MEDIUM

Chapter 1-A Performance Monitoring

The Department of Information Resources (Department) complied with applicable requirements in monitoring the two Data Center Services (DCS) contracts selected for review: (1) Texas Private Cloud, Facilities and Computing Services (Texas Private Cloud) and (2) Technology Solution Services. However, the Department should strengthen user access controls over its contract management system.

The Department had adequate processes and controls for monitoring performance.

As required by the *State of Texas Procurement and Contract Management Guide* for high-dollar and high-risk contracts, the Department established enhanced monitoring procedures for its Shared Technology Services contracts. The two contracts audited included multiple deliverables, expected service levels, and meetings with contractors. The Department employed contract managers and vendor managers with required certifications to oversee the contracts and reported the contractors' performance to the Office of the Comptroller of Public Accounts (Comptroller's Office) as required by Title 34, Texas Administrative Code, Section 20.115. (See text box for details about vendor performance tracking.)

Vendor Performance Tracking

The Comptroller's Office's Statewide Procurement Division maintains a vendor performance tracking system on its web page to publish vendor performance reports and vendor grades submitted by state agencies. State agencies must submit a performance report and grade within 30 days of the completion of a key milestone identified in the contract and at least once each year during the term of the contract, if the contract value exceeds \$5 million.

Source: Title 34, Texas Administrative Code, Sections 20.115 and 20.509

Deliverables. For the eight Texas Private Cloud and six Technology Solution Services deliverables tested, the Department employed staff with contracting and technical knowledge to review deliverables. The sampled deliverables met minimum acceptance criteria established by the Department.

Expected Service Levels. For all 10 service level results tested for both the Texas Private Cloud and Technology Solution Services contracts, the reported service level was calculated accurately. Additionally, a service level improvement plan was created for any underperformance at the critical service level during the scope, as required by the contracts.

Owner-operator Governance Structure. The Department established communication channels to enable customers to provide information about potential issues and scheduled regular meetings with the contractors.

- **Monthly Customer Surveys.** From September 1, 2020 through December 31, 2022, the average response rate was 75 percent for the Texas Public Cloud contract and 76 percent for the Technology Solution Services contract. For all 22 Texas Private Cloud responses and all 4 Technology Solution Services responses requiring service requests that were tested, requests were created and resolutions identified.
- **Governance Meetings.** The Department scheduled weekly meetings with the contractors and bi-monthly meetings with customer and contractor representatives. While some meetings were canceled, as the Department asserted they were determined not to be necessary, it consistently met with contractors and customers and documented meetings during the three months tested.

The Department should strengthen user access controls for its contract management system.

The Department did not perform periodic user access reviews of its contract management system. Texas Administrative Code, Title 1, Section 202.22, requires information owners or designated representatives to be responsible for approving access to information resources and periodically reviewing access lists based on documented risk management decisions. The Department took appropriate steps to correct issues identified during testing. Details related to user access issues were communicated to the Department separately in writing.

Recommendations

The Department should:

- Establish periodic reviews of user access to its contract management system, based on documented risk management decisions.
- Ensure that user access to its contract management system aligns with job duties and that access is removed promptly when staff or contractors leave employment.

Management's Response

DIR agrees with the recommendations and will implement them as follows:

DIR Information Technology Services (ITS) will conduct quarterly reviews of all users in our contract management system to ensure any separated employees and contractors have been deactivated. In addition, ITS will conduct semi-annual reviews of all user access to confirm that the job duties of existing employees and contractors continue to support the appropriate access levels. The DIR personnel overseeing necessary business units will be consulted to confirm the levels of access for all such employees and contractors. ITS will schedule the reviews as a recurring meeting on the calendars of the ITS Application Delivery Manager, ITS Help Desk Manager, and necessary business units.

Implementation Date: September 1, 2023

LOW

Chapter 1-B Fiscal Monitoring

The Department had adequate processes and controls for monitoring payments and invoices.

Payments to Contractors. For both the Technology Solutions Services and Texas Private Cloud contracts, the Department paid invoices in accordance with its policy, contractual guidelines, and timeliness requirements.

For the six months tested for each contract, the Department ensured that critical service level performance agreements were met, required deliverables were submitted, and vendor invoice review checklists were properly completed. Additionally, invoices were approved by the financial team and the vendor management team before payment. The contractor payments were supported by contractor invoices, and payments were made within 30 days as required by Texas Government Code, Section 2251.021.

Customer Invoices. The Department's processes and controls worked effectively to ensure that invoices provided to customers by the Department were based on services purchased or consumed and that services and rates were allowable and matched the rates in the contracts. Additionally, all customers associated with a sampled invoice had an inter-agency or inter-local contract with the Department for the DCS program before the invoice was issued.

For all 32 invoices tested for the Technology Solutions Service contract and all 33 invoices tested for the Texas Private Cloud contract, the invoiced amounts matched information from the chargeback system administered by the multi-sourcing services integrator, Capgemini.¹

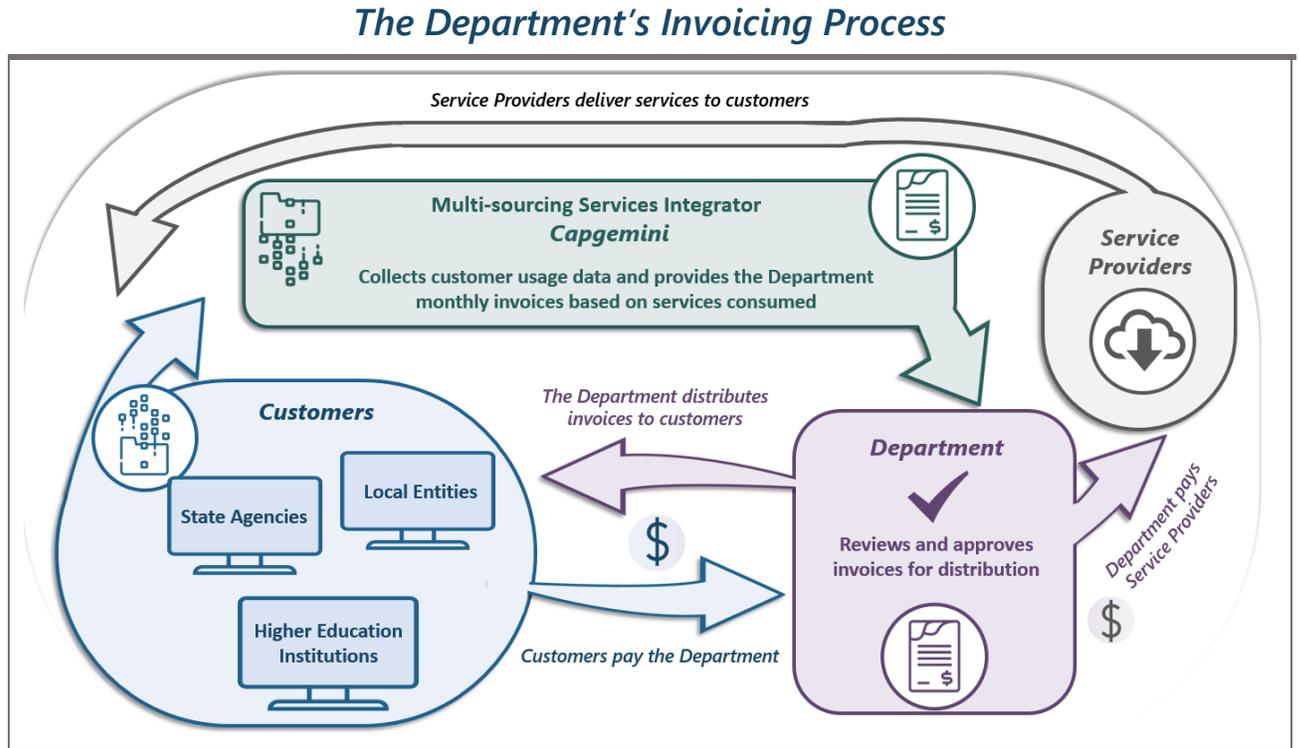
For line items tested in the associated invoices, all pricing matched amounts listed in the contracts or approved custom quotes. Additionally, for the Technology Solutions Service contract, the Department reviewed application

¹ This audit did not perform any work on the chargeback system administered by Capgemini. Auditors reviewed the *Capgemini America, Inc. Multi-Sourcing Services Integrator Chargeback System for the State of Texas Department of Information Resources System and Organization Controls (SOC) for Service Organization Report for the period of September 1, 2021, to August 31, 2022*, to gain reasonable assurance about the controls for the chargeback system.

development tickets to ensure that purchased services used DCS infrastructure, as required.

Figure 3 and the text box below show how the Department’s invoicing process works.

Figure 3



Source: Information provided by the Department.

Invoicing Process

As the multi-sourcing services integrator (MSI), Capgemini administers the invoicing and chargeback process, which accounts for costs incurred by the MSI, service component providers, and customers each month. Customers agree to pay the Department applicable charges for services received from the contractors and the MSI, including Department recovery fees of 2.95 percent, any allocated charges, and any pass-through expenses incurred. Each month, the MSI provides invoices to the Department.

The Department reviews and approves the costs identified by the invoicing process and sends invoices to customers. After customers pay the Department, the Department pays contractors.

Source: The Department.

NOT RATED

Chapter 2 Prior Recommendations

The Department substantially implemented one recommendation; corrective action is incomplete or ongoing for two others.

The State Auditor’s Office selected and reviewed the implementation statuses for three recommendations from prior State Auditor’s Office audit reports. The Department self-reported that it had fully implemented all three of those recommendations.

Board training in contracting. Auditors determined that the Department has **substantially implemented** a recommendation from [An Audit Report on a Selected Contract at the Department of Information Resources](#) (SAO Report No. 21-018, May 2021) related to required training in contracting for board members.

Asset management. Auditors determined that corrective action is **incomplete or ongoing** for two recommendations from [An Audit Report on Financial Processes at the Department of Information Resources](#) (SAO Report No. 20-029, April 2020) related to asset management and media sanitization of assets.

Figure 4 on the next page shows the implementation status determined by auditors for each of the recommendations, along with comments explaining the determination.

Definition of Implementation Status
Each implementation status is defined as follows:

-  **Fully Implemented:** Successful development and use of a process, system, or policy to implement a recommendation.
-  **Substantially Implemented:** Successful development but inconsistent use of a process, system, or policy to implement a recommendation.
-  **Incomplete or Ongoing:** Ongoing development of a process, system, or policy to address a recommendation.
-  **Not Implemented:** Lack of a formal process, system, or policy to address a recommendation.
-  **Not Applicable:** N/A signifies that the recommendation is no longer applicable.

Figure 4

Summary of State Auditor’s Office Determinations of the Implementation Status of Selected Prior Audit Recommendations

Recommendations	Implementation Status Determined by Auditors
<p><i>An Audit Report on a Selected Contract at the Department of Information Resources</i> SAO Report No. 21-018, May 2021, Chapter 3</p> <p style="text-align: right;">Rating: Medium ●</p>	
<p>The Department should ensure that all board members complete the required contract training.</p> <p>Auditor Comments: The Department implemented a spreadsheet to track the status of board members’ training; however, it did not ensure that all board members had completed the training in contracting required by Texas Government Code, Chapters 656 and 2054, and by the Department’s <i>Board Training Guide</i>. Of the 10 board members active in January 2023 who were due to have training in contracting before March 1, 2023, 4 (40 percent) had not completed the required training.</p>	
<p><i>An Audit Report on Financial Processes at the Department of Information Resources</i> SAO Report No. 20-029, April 2020, Chapter 4</p> <p style="text-align: right;">Rating: Priority ●</p>	
<p>To strengthen its processes for tracking and securing assets, the Department should ensure that accurate asset information is recorded in the State Property Accounting System (SPA), including:</p> <ul style="list-style-type: none"> • Verifying that asset locations are recorded correctly in SPA and updating that information in a timely manner when asset locations change. • Entering assets in SPA at the time of acquisition. • Updating SPA accurately and timely for changes to active assets and for disposals. 	

Recommendations

Implementation
Status Determined
by Auditors**Auditor Comments:**

The Department has implemented a process to ensure that asset acquisitions are recorded in SPA. For 13 (93 percent) of 14 asset acquisitions tested, the received dates and in-service dates recorded in SPA were accurate. Although the Department implemented some new asset tracking processes, testing of samples of active assets identified that those processes were not adequate to ensure that the asset information was accurate in SPA, as required by Texas Government Code, Section 403, and the Comptroller's Office *SPA Process User's Guide*. Specifically, for 25 assets recorded as active in SPA that were randomly selected for testing:

- 17 (68 percent) were recorded correctly.
- 8 (32 percent) had incorrect information in fields for asset tag, custodian, location, or serial number. Of those 8, 5 were inactive and recorded as active in error; 4 of those 5, including 2 that had been decommissioned in June 2020, could not be located.

An additional 27 assets that were listed as active but had been decommissioned were identified through data analysis. Auditors also tested five assets selected using a risk-based methodology; these assets were correctly recorded in SPA.

To strengthen its processes for tracking and securing assets, the Department should perform and document media sanitization before an asset is disposed or transferred as required by its *Security Controls Catalog*.

**Auditor Comments:**

The Department was not ensuring that media sanitization is documented for all asset disposals and transfers, as required by the Department's *Security Controls Standards Catalog*, version 2.0. Specifically:

- The Department has not developed procedures to document media sanitization for asset transfers. As a result, for all 12 (100 percent) of the asset transfers tested, there was no documentation to support that the media sanitization was performed.
- The Department has developed a process to document media sanitization for disposals; however, that process was not always followed. Of 3 assets randomly selected, 1 (33 percent) did not have documentation to support that the media sanitization was performed. Auditors also tested four assets selected using a risk-based methodology; those assets had documentation of the media sanitization performed.

Management's Response

DIR agrees with the recommendations and will implement them as follows:

The IT Services (ITS) department has updated the documentation process of asset tracking to include the sanitation of assets before internal transfer.

DIR believes its policies and procedures for many asset management tasks were sufficient to ensure the necessary tasks are performed; however, DIR believes that failures to follow those procedures resulted from having responsibility for IT asset (laptops, tablets, etc.) management placed on staff in DIR's Chief Financial Office, while the assets in question are being handled and distributed by staff in the Chief Technology Office. DIR now sees that structure was inefficient because the staff with knowledge and control over IT assets were not responsible for documentation of the activities, such as sanitization, they performed. As a result, DIR management has reassigned formal responsibility for IT asset management to the ITS team. To ensure those assets are adequately tracked, staff within the Chief Financial Office will continue to manage the State Property Accounting (SPA) records by comparing DIR's internal records to the SPA records and working with ITS to resolve any discrepancy between the two records. In addition, DIR's Internal Audit department will periodically select a sample of assets and physically verify that the device is possessed by the recorded custodian to which it is assigned. DIR is also investigating new custodian tracking software to further document the asset lifecycle.

Implementation Date: September 1, 2023



Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Department of Information Resources (Department) has processes and related controls to help ensure that selected Data Center Services contracts are monitored in accordance with applicable requirements.

Scope

The scope of this audit included the Department’s contract monitoring activities from September 1, 2020, through December 31, 2022, for two contracts: (1) Texas Private Cloud, Facilities and Computing Services with the Atos Government IT Outsourcing Services LLC, and (2) Technology Solution Services with Deloitte Consulting LLP. The scope also included a review of significant internal control components related to the Department’s contract monitoring processes for the two contracts selected. This audit did not involve any work with customers or with other service component providers. It did not include tests to determine whether contractors complied with significant terms of the two selected contracts, other than the contractors’ participation in monitoring processes established in the contracts and their compliance with the Department’s policies and procedures.

The following members of the State Auditor’s staff performed the audit:



- Anna Howe, CFE (Project Manager)
- Rachel Lynne Goldman, CPA, CISA, CFE (Assistant Project Manager)
- Rogelio De La Fuente Jr., CPA
- Douglas Jarnagan, MAcc
- Kevin Mack
- Emmanuel Melendez, CPA, CIA, CFE
- Elizabeth N. Padilla, CPA
- Alexander Sumners
- Robert G. Kiker, CFE, CGAP (Quality Control Reviewer)
- Michael A. Simon, MBA, CGAP (Audit Manager)

The scope also included the corrective actions that the Department implemented to address selected recommendations from [An Audit Report on a Selected Contract at the Department of Information Resources](#) (SAO Report No. 21-018, May 2021) and [An Audit Report on Financial Processes at the Department of Information Resources](#) (SAO Report No. 20-029, April 2020).

Methodology

We conducted this performance audit from November 2022 through July 2023 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. In addition, during the audit, matters not required to be reported in accordance with *Government Auditing Standards* were communicated to the Department's management for consideration.

Addressing the Audit Objectives

We selected the two Data Center Services contracts for this audit based on risk factors identified by auditors and contract values.

Additionally, we performed the following:

- Determined whether the Department had adequate controls over contract monitoring to ensure compliance with requirements in Texas Government Code, Chapters 2054, 2155, 2157, 2251, 2261, and 2262; Texas Administrative Code, Title 1, Sections 201 and 202, and Title 34, Section 20; the *State of Texas Procurement and Contract Management Guide*, version 2.1; and the Department's *Security Control Standards Catalog*, version 2.0, by:
 - Reviewing the Department's policies and procedures.
 - Interviewing Department staff to gain an understanding of contract monitoring for the selected contracts, including internal controls and information that supports those processes.

- Reviewing the Department’s contract monitoring design, contract manager and vendor manager qualifications, risk assessments, and required reporting for the selected contracts.
- Testing samples to determine if performance and fiscal monitoring procedures were occurring according to the contracts and Department policies and procedures.
- Performing limited general controls testing, including reviewing a risk-based selection of user access accounts and profiles in the contract management system; assessing the Department’s semiannual user access review of the Centralized Accounting and Payroll/Personnel System (CAPPS); reviewing user access in CAPPS for segregation of duties for contract vendor payments; and reviewing Security Operations Center reports for service component providers.

Figure 5

Total Populations and Samples Selected for Testing Contract Monitoring

Population ^a	Population Size ^{bc}	Sample Size ^{bc}	Sampling Methodology
Customer Survey Responses That Required Action	Cloud: 218 Solution: 34	Cloud: 22 Solution: 4	Selected a nonstatistical sample through random selection. ^d
Required Contract Deliverables	Cloud: 76 Solution: 54	Cloud: 8 Solution: 6	Selected nonstatistical samples for testing to ensure coverage of recurring deliverables related to security and technology. ^e
Reported Service Level Agreements	Cloud: 21 Solution: 19	Cloud: 5 Solution: 5	Selected nonstatistical samples for testing to gain coverage of recently assessed service level agreements and service level agreements that had performance issues. ^e
Governance and Solution Group Meetings	Cloud: 28 months Solution: 28 months	Cloud: 3 months Solution: 3 months	Selected nonstatistical samples for testing to ensure coverage of meetings during months that service level agreements were not met; the meetings within those months were reviewed. ^e
Vendor Payments	Cloud: 28 Solution: 28	Cloud: 6 Solution: 6	Selected a nonstatistical sample using random selection. ^d

Population ^a	Population Size ^{bc}	Sample Size ^{bc}	Sampling Methodology
Customer Invoice Line Items	Cloud: 10,280 Solution: 1,615	Cloud: 25 Solution: 25	Assembled a nonstatistical sample of customer invoices by randomly selecting monthly invoices; additionally reviewed support of the highest line item amount on the monthly invoices tested. ^e
Customers With Charges Over \$1,000	Cloud: 43 Solution: 36	Cloud: 8 Solution: 7	Selected nonstatistical samples for testing to ensure coverage of customers with total payments over \$10 million and large fluctuations in payments. Tested the month with the largest payment amount and reviewed support of the highest line item amount on the monthly invoices selected. ^e

^a The populations included data from the period between September 1, 2020, and December 31, 2022.

^b “Cloud” is the Texas Private Cloud, Facilities and Computing Services contract with Atos Government IT Outsourcing Services, LLC.

^c “Solution” is the Technology Solution Services contract with Deloitte Consulting LLP.

^d A nonstatistical random sample is representative. This sample design was chosen so the sample could be evaluated in the context of the population. It would be appropriate to project those test results to the population, but the accuracy of the projection cannot be measured.

^e The sample items chosen to ensure coverage of specific characteristics identified in the population were not necessarily representative of the population; therefore, it would not be appropriate to project the test results to the population.

- **Prior Recommendations:** Determined whether the Department implemented the recommendations from [An Audit Report on a Selected Contract at the Department of Information Resources](#) (SAO Report No. 21-018, May 2021) and [An Audit Report on Financial Processes at the Department of Information Resources](#) (SAO Report No. 20-029, April 2020) by:
 - Reviewing the training tracking spreadsheet and supporting documentation to determine if all board members completed the required training in contracting.
 - Testing samples, as described in Figure 6 on the next page, to determine if the Department was ensuring that accurate asset information was recorded in the State Property Accounting System (SPA) and that there was documentation of media sanitization for asset disposals and transfers.

Figure 6

**Total Populations and Samples Selected
for Prior Audit Recommendations**

Population	Population Size	Sample Size	Sampling Methodology
Active Assets in SPA	1,246	30	Selected a nonstatistical sample of 5 for testing based on risk to ensure coverage of assets (1) located at the state data centers and (2) with no custodian recorded. ^b Selected an additional nonstatistical sample of 25 using random selection. ^a
Asset Acquisitions in SPA	71	14	Selected a nonstatistical sample using random selection. ^a
Asset Disposals in SPA	19	7	Selected a nonstatistical sample of four for testing based on risk to ensure coverage of (1) information technology assets and (2) assets placed in service after September 1, 2022. ^b Selected an additional nonstatistical sample of three using random selection. ^a
Information Technology Asset Transfers in the Asset Tracker	78	12	Selected a nonstatistical sample of 12 for testing based on risk to ensure coverage of (1) transfers between different types of custodians and (2) assets with surplus designation. ^b

^a A nonstatistical random sample is representative. This sample design was chosen so the sample could be evaluated in the context of the population. It would be appropriate to project those test results to the population, but the accuracy of the projection cannot be measured.

^b The risk-based sample items were chosen to address specific risk factors identified in the population. A risk-based sample is not representative, and it would not be appropriate to project those test results to the population.

Data Reliability and Completeness

To determine data reliability and completeness, auditors (1) observed the Department’s extraction of requested data populations, (2) reviewed data queries and report parameters, (3) compared totals between information technology systems, (4) reviewed reasonableness of data in key fields, and (5) conducted testing of user access for CAPPs and the Contract Management System.

Auditors determined that the following data sets were sufficiently reliable for the purposes of the audit:

- **CAPPS:** Payments to vendors.
- **Information Technology Financial Management system:** Customer invoice detail.
- **Information Technology Service Level Management system:** Performance metrics for service level agreements.
- **Contract Management System:** Contract deliverables and approvals.
- **ServiceNow:** Customer service surveys' responses and recipients.
- **Asset Tracker:** Information technology asset transfers.

As discussed in Chapter 2, the active asset, asset acquisition, and asset disposal data in **SPA** was not always reliable; however, this data was the most complete information available, and auditors used the data for the purposes of this audit.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Appendix 2

Related State Auditor's Office Reports

Figure 7

Report Number	Report Name	Release Date
22-035	<i>A Report on the Implementation Status of Prior State Auditor's Office Recommendations</i>	July 2022
21-018	<i>An Audit Report on a Selected Contract at the Department of Information Resources</i>	May 2021
20-029	<i>An Audit Report on Financial Processes at the Department of Information Resources</i>	April 2020
17-038	<i>An Audit Report on Selected Contracts at the Department of Information Resources</i>	June 2017



Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair

The Honorable Dade Phelan, Speaker of the House, Joint Chair

The Honorable Joan Huffman, Senate Finance Committee

The Honorable Robert Nichols, Member, Texas Senate

The Honorable Greg Bonnen, House Appropriations Committee

The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Department of Information Resources

Members of the Department of Information Resources Governing Board

Ms. Amanda Crawford, Executive Director



This document is not copyrighted. Readers may make additional copies of this report as needed. In addition, most State Auditor's Office reports may be downloaded from our website: <https://sao.texas.gov>.

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9500 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD); or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government, visit <https://sao.fraud.texas.gov>.