DATASCAN

Contract Datascan LP's Full Service Inventory Capture and Reporting System

– Report on Contract Datascan LP's Description of its Full Service Inventory Capture and Reporting System and on the Suitability of the Design and Operating Effectiveness of its Controls

– System and Organization Controls (SOC) – SOC 1 Type 2 Report

– For the Period May 1, 2024, to October 31, 2024

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

bakertilly

Contents

1. Independent Service Auditor's Report

To the management of Contract Datascan, LP:

Scope

We have examined management of Contract Datascan, LP's (Datascan) description of its Full Service Inventory Capture and Reporting System, entitled "Contract Datascan, LP's Description of its Full Service Inventory Capture and Reporting System" for processing user entities' transactions throughout the period of May 1, 2024, to October 31, 2024 (description), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of Contract Datascan, LP's Management" (assertion). The controls and control objectives included in the description are those that management of Datascan believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Full Service Inventory Capture and Reporting System that are not likely to be relevant to user entities' internal control over financial reporting.

Datascan uses subservice organizations to provide cloud hosting services and colocation services. The description includes only the control objectives and related controls of Datascan and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Datascan can be achieved only if complementary subservice organization controls assumed in the design of Datascan's controls are suitably designed and operating effectively, along with the related controls at Datascan. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Datascan's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 2, management of Datascan has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Management of Datascan is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period of May 1, 2024, to October 31, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- Evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in management of Datascan's assertion,

a. The description fairly presents the Full Service Inventory Capture and Reporting System that was designed and implemented throughout the period of May 1, 2024, to October 31, 2024.

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period of May 1, 2024, to October 31, 2024, and the subservice organizations and user entities applied the complementary controls assumed in the design of Datascan's controls throughout the period of May 1, 2024, to October 31, 2024.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period of May 1, 2024, to October 31, 2024, if complementary subservice organizations and user entity controls assumed in the design of Datascan's controls operated effectively throughout the period of May 1, 2024, to October 31, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Datascan, user entities of Datascan's Full Service Inventory Capture and Reporting System during some or all of the period of May 1, 2024, to October 31, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Baker Tilly US, LLP

Frisco, Texas
November 26, 2024

2. Assertion of Contract Datascan, LP's Management

We have prepared the description of Contract Datascan, LP's (Datascan) Full Service Inventory Capture and Reporting System entitled "Contract Datascan, LP's Description of its Full Service Inventory Capture and Reporting System," for processing user entities' transactions throughout the period of May 1, 2024, to October 31, 2024 (description) for user entities of the system during some or all of the period May 1, 2024, to October 31, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented at the subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Datascan uses subservice organizations to provide cloud hosting services and colocation services. The description includes only the control objectives and related controls of Datascan and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Datascan can be achieved only if complementary subservice organization controls assumed in the design of Datascan's controls are suitably designed and operating effectively, along with the related controls at Datascan. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Datascan's controls are suitably designed and operating effectively, along with related controls at Datascan. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Full Service Inventory Capture and Reporting System made available to user entities of the system during some or all of the period May 1, 2024, to October 31, 2024, for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting.

   The criteria we used in making this assertion were that the description:

   i.   Presents how the Full Service Inventory Capture and Reporting System made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable,

        (1)   The types of services provided, including, as appropriate, the classes of transactions processed.

        (2)   The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

        (3)   The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

        (4)   How the system captures and addresses significant events and conditions, other than transactions.

(5)   The process used to prepare reports or other information provided to user entities.

(6)   Services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7)   The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

(8)   Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii.   Includes relevant details of changes to the service organization's system during the period covered by the description.

iii.   Does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the Full Service Inventory Capture and Reporting System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period May 1, 2024, to October 31, 2024, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of Datascan's controls throughout the period May 1, 2024, to October 31, 2024. The criteria we used in making this assertion were that:

i.   The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii.   The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii.   The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

3. Contract Datascan, LP's Description of its Full Service Inventory Capture and Reporting System

Overview of Company

Contract Datascan, LP ("Datascan" or "the Company") is a Texas limited partnership providing inventory-counting solutions and consulting for retailers worldwide. Its principal place of business is in Carrollton, Texas.

Barcode Inventory Counting Solution

Datascan offers self-scan and full-service barcode inventory counting. The self-scan barcode inventory counting solution offers customers a technology solution, DART, that is configured to client specifications. The client is trained by Datascan on the technology, which is then utilized by the client's staff to perform the inventory count. For self-scan clients, the client is responsible for the accuracy, performance, processes and procedures of the count execution. Datascan offers staff augmentation resources to self-scan clients to assist with inventory counts as needed.

The full-service barcode inventory counting solution is a technology solution, DART, that is configured to the client's specifications as well as a labor solution. Unlike self-scan, Datascan provides the staffing to perform the count utilizing the Datascan technology and processes. Datascan is responsible for the accuracy and productivity of the count leveraging the processes and procedures defined in conjunction with the client.

Datascan also offers an RFID inventory counting solution leveraging a third party software platform, OCTO+. Datascan will resell and install hardware, configure OCTO+, and provide the necessary training and support for clients to use in their business operations.

Scope of the Description

This report is intended to provide an understanding of the controls over the Full Service Inventory Capture and Reporting System procedures for full-service barcode inventory solution in relation to user entities' controls over financial reporting. It is not intended to cover the RFID Inventory Capture Solution. Datascan uses employees and third-party resources to perform full-service counts. Datascan has responsibility and oversight over the count process and the resources executing the counts. The content of this report is designed to provide information to user organizations and auditors of such user organizations in assessing control risk.

Datascan uses various subservice organizations to support its Full Service Inventory Capture and Reporting System. The description includes only the control objectives and related controls of Datascan and excludes the control objectives and related controls of the subservice organizations.

Subservice Organization	Type of Service	Specific Service Provided
CyrusOne, LLC (CyrusOne)	Colocation data center services	Colocation which houses the data center for components of DART not migrated to Azure.
Microsoft Azure	Cloud hosting services and IT Services	Microsoft technology is used for hosting the web application, cloud hosting services, and identity and access management.

Internal Control Framework

This section provides information about the five interrelated components of control at Datascan, including

- control environment,

- risk assessment,

- monitoring activities, and

- information and communication

Control Environment

Organization

The Datascan organization consists primarily of the following groups:

Sales & Marketing - interacts directly with prospective clients to contract and onboard new clients and new requirements. Client Services typically manages the client relationship after a contract is signed. Client Services interacts directly with existing clients and handles all communications with the client during the self-scan inventory process. Client Services also interacts with Operations and Information Technology. The Chief Revenue Officer reports to the Company's President.

Inventory Solutions and Sales – interacts with Sales & Marketing to scope the full-service staffing and process requirements and partners with Human Resources and third-party vendors to staff the count operations. The Inventory Solutions and Sales group is responsible for executing client count operations as well as all staffing logistics. The team is responsible for sales, contracting, implementing, and training of RFID solutions. The VP of Inventory Solutions reports to the Chief Revenue Officer.

Operations - interacts with Sales & Marketing, Client Services, and IT Solutions Delivery. The Operations group is responsible for order fulfillment, shipping/receiving, logistics, quality control, billing, and resource planning. The Vice President of Global Operations reports to the Company's President.

Information Technology - interacts with Operations, Inventory Solutions and Sales, Sales & Marketing, Client Services, Human Resources, and Finance & Accounting. This group develops and supports the DART application, corporate systems, internal desktop network, and telephone systems. This group is responsible for the design and manufacturing oversight of the Company's scanner fleet. Information Technology also operates a 24-hour Call Center that supports self-scan, full-service, and RFID. The Chief Information Officer reports to the Company's President.

Finance & Accounting – interacts with all departments managing the financials of the Company. This group is responsible for ordering and invoicing of client contracts. The Chief Financial Officer reports to the Company's President.

Human Resources – interacts with all departments to manage the employee lifecycle, own Personnel Policies and Procedures, and perform payroll and benefits functions. The Sr. Director, Human Resources reports to the Company's President.

Management Control

The President, who is actively involved in the Company's day-to-day operations, establishes the control environment at Datascan. All employees are required to understand the President's mandate for a thorough control environment. The Company's President meets regularly with the responsible direct reports to stay abreast of issues. In turn, each direct report meets regularly with his or her personnel to communicate activities, challenges, and risks.

Personnel Policies and Procedures

Datascan has formal hiring practices designed to ascertain if potential employees are qualified for their responsibilities. The appropriate leaders must approve all new employees. Hiring policies include experience, education requirements, and reference checks. Any new employee who has access to any systems and/or applications are subject to background checks.

All new employees complete a new hire package which includes a confidentiality agreement and a policy acknowledgment form. It is the responsibility of each Datascan manager to ensure all employees receive the necessary training to enable each employee to perform his or her duties.

In the event of terminations, closing interviews are conducted to cover insurance and other benefits and to ensure keys and security access cards are returned. Additionally, IT is notified of all terminated employees to appropriately change or revoke user identification codes.

Insurance

Datascan maintains insurance coverage through an outside carrier against major risk. Policies include personal and property damage, employee dishonesty, and general liability.

Risk Assessment

The Executive Leadership Team meets periodically to identify and manage risks which could affect the ability of Datascan to provide reliable inventory processing for its clients. The purpose of these meetings is to:

- Identify significant risks inherent in Datascan services;

- Identify the underlying sources of risk;

- Assess the impact of such risks to the Datascan client;

- Establish acceptable risk tolerance levels; and

- Implement appropriate measures to monitor and manage these risks.

As a normal course of operations, the management team monitors performance, quality, and controls. Technology quality control is performed by reviewing checklists attached to each order to ensure software and hardware configurations are shipped according to client specifications. Furthermore, operational issues encountered at the client site are logged and retained in a help desk tracking system. IT management monitors the performance and capacity levels of the systems and network on a regular basis. If sub-optimal performance and capacity measures are detected, IT management has a process in place to respond in a timely manner. Internal monitoring occurs in the form of periodic reviews conducted by Datascan employees.

Full-service quality control is performed by the Full-Service District Managers with periodic reviews by managers in the Inventory Solutions and Sales department.

Monitoring Activities

Daily operations are monitored through the use of the information and communication systems described below. Datascan management and supervisory personnel monitor the quality of internal controls as normal part of their activities. Monitoring software is used on the critical systems to monitor system performance and availability, and generates automatic alerts when certain protocols exceed thresholds relating to connectivity, processing capacity, and usage. (C04.01.01)

IT staff members are on call 24 hours a day during client inventories. Each on-call staff member is trained in system troubleshooting and recovery techniques.

Monitoring of Subservice Organizations

Datascan uses subservice organizations as defined above. Through its daily operational activities, management of Datascan monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively. Additionally, Datascan performs annual vendor reviews and reviews System and Organization Controls (SOC) reports for any inconsistencies and resolves issues, as necessary. (C03.03.03)

Information and Communication

Datascan has implemented different methods of communication to help ensure all personnel understand their individual roles and responsibilities over transaction processing and controls, and to help ensure significant events are communicated in a timely manner. These various direct and indirect methods of communication are implemented by management to ensure employees understand the policies, procedures, standards, and guidelines developed to define their individual roles and responsibilities. Examples of these methods include orientation and training for new employees, weekly team meetings, one-on-one meetings, performance reviews, emails, mobile messaging, ongoing training, distribution of policies and procedures and on-the-job training.

Users are provided with training manuals on how to perform scanning functions and are encouraged to communicate questions and issues to the appropriate training personnel. (C01.01.01) Every customer signs a customer contract which includes a service level agreement defining the organization's commitments and obligations to the customer and the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets. (C01.01.02)

Description of General Controls

Physical Security

The Company operates at Suite 100 at 2941 Trade Center Drive in Carrollton, Texas. The main entrance and side door to the building is locked during nonbusiness hours and opened only by an authorized access card. The Company maintains a list of active employees with active cards. The cards are de-activated as part of the termination process. All other outside doors are locked during non-business hours. Internal and external security cameras are motion-activated, and recordings are available for at least 30 but as long as 90 days depending on the camera's activity.   Approved visitors are escorted by authorized personnel. (C03.03.01)

Third-Party Colocation Data Center Facility

Datascan has contracted CyrusOne for data center and colocation services. Datascan houses some of their servers at CyrusOne facilities. The location is at 1649 W. Frankford Road, Carrollton, TX 75007. The perimeter of CyrusOne is monitored twenty-four hours a day by video surveillance cameras and security guards. Authorized individuals can access CyrusOne facility via a dual authentication process via a key card and biometric system. All visitors are required to provide photo identification to the security guards and electronically check-in through their electronic visitor system prior to entry. The data center personnel are on-site 24/7 for monitoring purposes. Approved visitors are escorted by authorized personnel or a security guard. These controls are the responsibility of CyrusOne and are not included within the scope of the report.

A two-factor electronic access authentication system, key card access and biometrics, and digital surveillance cameras are installed at the entrances and egresses of the data center. All Datascan equipment is housed in a biometrically locked cage and only authorized personnel have access to the locked cage. The colocation facility utilizes termination procedures which include revoking data center access upon notification from Datascan regarding employee termination. Datascan audits the key access list and the list of authorized user access additions, changes and removals logged by the colocation service provider for completeness and accuracy. (C03.03.02) Corrective action is taken as needed. Management monitors the data center provider to ensure the controls at the data center which could affect the Company are operating effectively.

Third-Party Cloud Data Center

Datascan leverages Microsoft's Azure cloud solutions for portions of the DART system. As part of the Microsoft Azure cloud solution, Datascan takes advantage of all the inherent security controls that are part of the Microsoft Azure cloud offering   Access controls consist of using the Microsoft active directory solution, Entra ID (formerly known as Azure AD) with multifactor authentication (MFA). All accounts are controlled using user-based access based on the multiple roles available within the Azure platform. All terminations and addition of accounts are done via notification via the Jira ticketing system with details on what actions and roles must be assigned, changed or removed.

Logical Access and Security

All users who have access to the system and/or applications are required to have an approved username and password (which must comply with Company policy). (C03.01.01)

Datascan computer systems are protected by a firewall appliance. The firewall requires multi-layer authentication for a valid and active user to get through the firewall to have access to Company systems and data. The credentials used for accessing the Company's firewall Microsoft Windows domain and DART are unique for each user to each individual system. (C03.01.03) The firewalls are configured to provide secure remote network access via a virtual private network (VPN) tunnel to authenticate users with secure access. (C03.01.04)

Approved new user access requests are initiated by the user's direct manager or the HR Department for new hires and contractors, and are submitted to the IT Department via a change request. (C03.02.01) Approved user access request change tickets resulting from an employee transfer or a change in a user's job role are initiated by the user's direct manager or the HR Department and are submitted to the IT Department via a change request. All network and system access levels are based on job roles. (C03.02.02) Administrative access with the ability to change or modify client data are limited to authorized personnel based on job roles. (C03.01.02) Termination request tickets are initiated by the user's direct manager or the HR Department, and are submitted to the IT Department via a change request to remove the user's access from the network and systems per company policy. (C03.02.03)

The DART system has a multi-level security system. This security system was put in place when DART was first installed and is updated regularly. DART access is assigned by task and by user. Access is assigned based on each individual's function so that only personnel handling applicable functions can input, view, or modify data relating to that function. Client user accounts are created, modified, or removed based on authorized change requests sent by the customer to a designated client service representative. (C03.02.04)

The access log for the DART system is periodically reviewed and updated by management on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request. (C03.02.05) Access to devices used in the field at client locations are secured with a username and password. (C03.01.01)

Datascan uses cloud email protection solutions for antivirus and spam filter hardware console to scan emails received from outside Datascan for viruses before forwarding the emails to the email server. Additionally, each Company computer has antivirus utilities active to detect malware. (C04.01.02)

Computer Operations

The DART system is running on cloud-hosted network servers running in Microsoft Azure. These servers are accessible only by IT department domain administrators. All production servers utilize RAID technology to test data integrity for the source and production code, which may reside on the servers. In addition, all client production and development data and source code is backed-up continuously.

The server processing exceptions are reviewed upon electronic notification when a problem is detected. The system is designed to be fully redundant to minimize downtime. (C07.01.01) Monitoring software is used on the critical systems to monitor system performance and availability, and generates automatic alerts when certain protocols exceed thresholds relating to connectivity, processing capacity, and usage. (C04.01.01)

IT staff members rotate an on-call schedule supporting 24 hours a day during client inventories. Each on-call staff member is trained in system troubleshooting and recovery techniques.

Program Change Control

The SDLC policy describes the responsibilities and procedures around design, acquisition, implementation, configuration, modification, and maintenance of DART components during the system development lifecycle (C02.01.01).

All client-related software change requests are documented in an industry standard ticketing system. The appropriate resources make any requested configuration or coding changes. For coding changes, the developers perform their work in a separate environment from the production servers and equipment and submit their completed work product for review and testing by the quality assurance resources. Revisions and versions of codes are secured, tracked, and archived using GIT. (C02.01.02)

The company utilizes third-parties to assist in colocation data center services and certain IT services. When third-parties are utilized for these services, Datascan discusses the scope and responsibilities for the third-party. Datascan Management also reviews the third-party's SOC report to ensure there are no control deficiencies which could affect Datascan.

Critical Changes

For critical changes (i.e. source code changes, application development/enhancement), changes are tracked through a ticketing system. The developers perform their work in a separate environment from the production servers. Once complete, the work is tested by a separate individual. If approved, another individual will move the change to the production live environment. If not approved, the work is sent back to the developer for further work and must be tested and approved prior to moving to a live environment.

Any changes (critical or non-critical) which require an emergency change must be reviewed and approved by a majority of the Change Advisory Board prior to implementing into production or within 72 hours from the time the change was moved to production. (C02.01.04) Emergency changes are tracked in the ticketing system and include a timely post implementation review. (C06.01.03) Procedures are in place for ensuring only reviewed and approved changes are made to production systems, including procedures for documenting, testing and authorizing code and database changes to the production environment prior to implementation. Separate test and production environments are maintained. The ability to migrate between development, test, and production environment is restricted to only authorized employees. (C06.01.04)

Key personnel are properly notified of any critical change releases to the DART system. (C02.01.03)

Change Management

For all other changes (not deemed critical), the Company's policy defines the documentation and authorization of software and hardware changes to the system. The policy states these changes must be reviewed and approved prior to movement into the production environment. These changes are also tracked in the ticketing system. The DART system is configured to automatically record changes to objects. (C02.01.06)

The Company has the same process in place as noted above for non-emergencies. (C06.01.01) System change requests (i.e. infrastructure changes) not classified as minor are evaluated and approved to determine the potential effect of the change throughout the change management process. (C06.01.02)

Employees with the ability to migrate between the development, test, and production environment are reviewed and approved by executive management on at least an annual basis to ensure privilege user access is only provided to the minimum number of employees in which privileged access is necessary to carry out their job responsibilities. (C02.01.05)

Incident Management

The Company has a policy in place that describes the responsibilities and procedures of management and customers in the event of a system security breach or complaint and includes steps to be taken to coordinate the Company's response and remediation from such situations. (C.05.01.01) Internal incidents are tracked through the ticketing system which documents the appropriate items of each incident. (C05.01.02) Furthermore, the Company utilizes a documentation repository to assist in resolving incidents. Technical reference documents are available to assist personnel in the resolution of common system processing errors and general troubleshooting. (C05.01.03)

Media and Disk Management

The Company has infrastructure components which have been designed so that all operationally critical components which have redundant counterparts are available to minimize downtime.

Datascan utilizes a real-time automated backup system which uploads all critical data on the company servers (such as processed client data files on a parallel database with failover capabilities). (C07.01.02) Client production data is backed up on at least a daily basis. (C07.01.04) Backups are monitored via an automated system that sends notifications to alert IT personnel when backups are not successfully completed and the incident management process is initiated accordingly. (C07.01.05)

The backup data is also electronically stored at a secure offsite data storage facility, to prevent the loss of critical data or system downtime from a destructive event. Client inventory data is retained in the system database for a minimum of 3 years. (C07.01.03)

Description of Inventory Processing

DART is configured to client requirements such as file integrations, reporting, count specifications, and timing. Datascan will provide the materials and equipment necessary to perform the count, such as fixture tags, scanners, and scanner accessories. Personnel must perform pre-count activities to prepare the store for the count to the client-defined defined processes and procedures. To perform the count, scanners are used to collect inventory data via scanned and keyed barcodes. The scanners may be Datascan devices or client devices running a Datascan android program. Once the scanning is complete, the data is loaded into the DART website where reporting is available for the appropriate party to monitor, support and correct the progress of their in-process inventories. Once count execution is complete, the store is closed, and post-inventory data analysis tools are available. Each client is provided count files in a format meeting the input requirements for their internal applications.

Description of Control Features by Function

Set Up a New Client

Program specifications for a new client are requested via a standardized form and captured in a ticketing system once analysis is completed by the appropriate resources upon clarification with the client. For customizations completed by the development team, the quality assurance team will perform the necessary testing prior to the production implementation. The Change Management procedures are followed to implement in production. The DART system does not allow inventory data to be uploaded into the system without completing the store setup process in order to verify all the required inventory setup information is completed before performing an inventory audit. (C09.01.01)

The Datascan count team leader is responsible for understanding and agreeing to client policies and procedures through written acknowledgment prior to leading a count. (C10.01.01) Starting September 8, 2024, the policy acknowledgment was implemented as an automated checklist item that was required to be completed before a count can be closed.

Staff the Count

Datascan provides the staff to take the inventory for client counts. Background checks are performed prior to onboarding for employees and contractors that perform full-service count services. (C10.02.01) All new employees and contractors that perform full-service counts are required to take training for proper performance of counting procedures. (C10.02.02)

Print and Ship Fixture Tags

Store fixture/zone tags are indexed with a sequential and unique number in order to identify and track inventory assets. (C09.01.03) All parameters used to print fixture tags come from the program specifications. Quality assurance processes are followed to ensure the tags meet specifications and requirements when printed. Area tickets are placed in accordance with client policies and procedures. (C10.01.08)

Prepare

The Datascan count team leader is responsible for loading client software on scanners and ensuring all quality procedures are followed prior to inventory count execution.

Take the Inventory

Personnel prepare the store for the count based on procedures previously provided by Datascan. Fixture tags are used in the stores when appropriate for ease of counting. DART scanners are used for the count. Inventory items are counted in accordance with client policies and procedures. (C10.01.07) Throughout the count, validation processes are used to assess the accuracy of the count. If there are issues, a recount may be required. Access to make adjustments, review amounts, and close an audit is restricted to authorized personnel. (C10.01.02) Inventory count adjustment reports are reviewed and approved according to the account policies and procedures as agreed to in the contract between Datascan and the applicable customer. (C10.01.03) Data received for store count data is systematically validated to ensure that data is complete and accurate. Issues are investigated and remediated. (C10.01.09) Prior to the close of an inventory count, any count adjustments made must have a rationale associated with the adjustment, as required by the customer. (C10.01.05) Every area tag must be accounted for before an inventory count can be closed. (C10.01.06) Once the personnel have completed the count, they are prompted to certify and close the inventory. Processes are in place to ensure that all physical locations were counted.

The DART system does not allow a store to close an inventory audit without an authorized user reviewing the system errors that resulted from the audit results and verifying all the system requirements for the inventory audit have been met prior to finalizing the inventory. (C09.01.02) The DART system restricts the ability to close an audit prior to completion of all tasks assigned for the store audit. (C10.01.04) Transmission of confidential information beyond the boundary of the system occurs through the secured communication technologies to protect communications between authorized parties. (C08.01.01) Data transmitted from the inventory scanners to the respective database is configured to be secured via encryption. (C08.01.02)

Monitor the Inventory

During the inventory count, Datascan personnel are available for count support. The DART system website is utilized for troubleshooting issues that are reported during a count either by an end-user or system notifications. Processes are defined and documented for handling issues that arise while conducting count operations.

Deliver the Count Files

The DART system produces a count file to client specifications. The files are created after a store closes its inventory. Inventory output files and reports are not generated before the inventory audit is closed in the DART system to ensure the inventory output files and reports sent to the client are accurate and complete. (C09.01.06) As stores close their inventories, the DART system verifies it has received all of the data from the

Host system. Any discrepancies halt the closing process. The appropriate on-call personnel are notified to address the issue.

Count files are delivered to clients in a secured transmission defined with the client during the specification phase. Inventory data uploads are recorded in the DART system via transaction event logs that can be reviewed by authorized users for system analysis or troubleshooting if needed. (C09.01.04) The DART system sends automatic email alerts to IT personnel when critical errors occur during the inventory data upload process in order to monitor issues and promote timely resolution. (C09.01.05)

Key Reports Provided to User Entities

Datascan provides inventory output files and reports to user entities related to the user entities' internal control over financial reporting.

Control Objectives and Related Controls

Datascan has specified the controls objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in Section 3 and 4 and are an integral component of Datascan's description of its Full Service Inventory Capture and Reporting System.

Complementary Subservice Organization Controls

Datascan's controls related to the Full Service Inventory Capture and Reporting System cover only a portion of overall internal control for each user entity of Datascan. It is not feasible for the control objectives related to Datascan's Full Service Inventory Capture and Reporting System to be achieved solely by Datascan. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with Datascan's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Complementary Subservice Organization Controls	Related Control Objective (CO)
CyrusOne, LLC	Physical access to the data centers is restricted to authorized personnel.	CO3.03
Microsoft	Physical access to the data centers is restricted to authorized personnel.	CO3.03
	Logical access to Microsoft infrastructure is restricted to authorized individuals.	CO3.01
	Backups are monitored for the successful completion and failures identified are reported and resolved.	CO7.01

Complementary User Entity Controls

Datascan's controls related to the Full Service Inventory Capture and Reporting System cover only a portion of internal control for each user entity of Datascan. It is not feasible for the control objectives related to the Full Service Inventory Capture and Reporting System to be achieved solely by Datascan. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with Datascan's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

– User entities are responsible for ensuring timely written notification of changes in the individuals authorized to instruct the Datascan client representative regarding activities on behalf of the client is provided to Datascan (CO 01.01 & CO 03.02).

– User entities are responsible for ensuring access to scanning equipment and upload terminals connecting to Datascan's DART system application is restricted to only those having the appropriate authorization (CO 03.01 and 03.02).

– User entities are responsible to ensure requests to manage access to Datascan's DART system application are authorized (CO 03.02).

– User entities are responsible for ensuring timely review of reports and notifying the Datascan client representative of discrepancies, if any (CO 05.01).

– User entities are responsible for selecting the appropriate encryption mechanism for file transfers (CO 08.01)

– User entities are responsible for changing password or access key to for file transfers (CO 03.01).

– User entities are responsible for ensuring that inventory data submitted to the DART system application is representative of the actual physical inventory for the client's location, that the inventory setup procedures have been completed appropriately by an authorized individual, and that the fixture listing is complete and accurate (CO 09.01).

– User entities are responsible for ensuring inventory procedures are re-performed by a supervisor or second individual on a sample of fixtures to verify that each item was counted only once and input data identified by the scanning equipment as erroneous is corrected prior to submission to Datascan's DART system applications (CO 09.01).

– User entities are responsible for ensuring edits to the counts or data are made by appropriate personnel and are accurate and complete (CO 09.01).

– User entities are responsible for ensuring output inventory reports are reviewed for completeness and accuracy by authorized client personnel (CO 09.01).

– User entities are responsible for ensuring output from programs is balanced routinely to relevant control totals (CO 09.01).

– User entities are responsible for ensuring inventory procedure is completed during the scheduled time and for only in-scope items (CO 09.01).

- The fixture listing and other data provided to Datascan for processing is complete and accurate (CO 10.01).

- Inventory recount procedures performed by the user entity are performed in accordance with user entity policies. (CO 10.01).

- Timely review of reports and notification of discrepancies, if any, is provided to the Datascan client representative (CO 10.01).

- Recount results provided by the user entity and recorded by Datascan are complete and accurate (CO 10.01).

- Output inventory reports are reviewed for completeness and accuracy by appropriate client personnel (CO 09.01 and 10.01).

- Output from programs is balanced routinely to relevant control totals (CO 09.01).

- User entities provide current count policies and procedures to Datascan (CO 10.01 and 10.02).

4. Description of Contract Datascan, LP's Control Objectives and Related Controls, and Baker Tilly's Description of Tests of Controls and Results

Information Provided by Baker Tilly

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at Datascan.

Our examination was limited to the control objectives and related controls specified by Datascan in Sections 3 and 4 of the report, and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate the information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, Datascan's controls may not compensate for such weaknesses.

Datascan's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by Datascan. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by Datascan, we considered aspects of Datascan's control environment, risk assessment, monitoring activities, and information and communication.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type of Test	Description
Inquiry	Inquiry of appropriate personnel and corroboration with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control
Re-performance	Reperformance of the control

In addition, as required by paragraph .36 of AT-C section 205, Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests
Communications		
Control Objective 1.01: Controls provide reasonable assurance that the responsibilities of internal and external users responsible for accessing, processing, communicating, or managing the organization's information and information assets that may affect user entities' internal control over financial reporting are defined and communicated.		
01.01.01 Client training manuals are available to system users as a step-by-step guide on how to perform the scanning functions required to complete an inventory audit as well as who to contact if they have questions or issues.	Inspected client training manuals to determine whether a step-by-step guide on how to perform the scanning functions required to complete an inventory audit was available and management communicated how to report incidents, concerns, and other complaints to the Company's personnel.	No exceptions noted.
01.01.02 Every customer signs a customer contract which includes a service level agreement defining the organization's commitments and obligations to the customer and the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.	For a sample of customers, inspected contract and supporting documentation to determine whether management communicated the Company's commitments and obligations to its customers via master service agreements.	No exceptions noted.
Application and System Development		
Control Objective 2.01: Controls provide reasonable assurance that the implementation of and changes to application programs with respect to user entities' internal control over financial reporting are authorized, tested, documented, approved, and implemented to result in complete and accurate reporting of transactions.		
02.01.01 The Company utilizes a policy describing the responsibilities and procedures around design, acquisition, implementation, configuration, modification, and maintenance of system components during the SDLC.	Inspected the SDLC Policy to determine whether the design, acquisition, implementation, configuration, modification, and maintenance of system components during the system development lifecycle were outlined and documented.	No exceptions noted.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests

Application and System Development

Control Objective 2.01: Controls provide reasonable assurance that the implementation of and changes to application programs with respect to user entities' internal control over financial reporting are authorized, tested, documented, approved, and implemented to result in complete and accurate reporting of transactions.

02.01.02	Procedures are in place for ensuring only reviewed and approved changes are made to production systems. These procedures include: • Documenting, testing, and authorizing code and database changes to the production environment prior to implementation • Separate test and production environments • Logical access procedures restrict the ability to migrate between development, test, and production environment to only authorized employees	For a sample of changes, inspected SDLC change tickets to determine whether the code changes were documented, authorized, and tested prior to being implemented into production. Inspected the development, test, and production environments to determine whether the development and test environment was segregated from the production environment. Inspected the list of authorized users to determine whether only authorized employees had access to both the development and production environments.	No exceptions noted.
02.01.03	Key personnel are properly notified of any critical database change releases to the DART system.	Inspected the system configuration settings to determine whether the system was set up to send notifications once critical changes were released to production.	No exceptions noted.
02.01.04	Procedures are in place to document and track emergency changes (hot fixes) to the production environment and include a timely post-implementation review within 24 to 72 hours of release, based on Company policy.	For a sample of emergency changes, inspected change tickets to determine whether the change requests were documented, authorized, and included a timely post implementation review.	No exceptions noted.
02.01.05	Employees with the ability to migrate between the development, test, and production environment are reviewed and approved by management on at least an annual basis to ensure privilege user access is restricted to employees based on job responsibilities.	Inspected the annual review of privileged employees to determine whether access for employees with the ability to migrate between the development, test, and production environment was reviewed by management on an annual basis to ensure access was limited based on job responsibilities.	No exceptions noted.

Controls Specific by Contract Datascan, LP		Tests Performed by Baker Tilly	Results of Tests
Application and System Development			
Control Objective 2.01: Controls provide reasonable assurance that the implementation of and changes to application programs with respect to user entities' internal control over financial reporting are authorized, tested, documented, approved, and implemented to result in complete and accurate reporting of transactions.			
02.01.06	The DART system is configured to automatically record changes to objects.	Inspected the DART system log to determine whether changes to objects were automatically recorded by DART.	No exceptions noted.
Logical and Physical Access Controls			
Control Objective 03.01: Controls provide reasonable assurance that logical access to programs, data, applications, and computer resources that may affect user entities' internal control over financial reporting is restricted to authorized users and such users are restricted to performing authorized actions.			
03.01.01	Unique identifier (user ID) and passwords are used to verify the identity and authentication of users. Additionally, password security requirements and parameters are in place to provide the standards to protect the Company's system components.	Inspected the passwords settings to in-scope systems to determine whether password parameters included minimum length, complexity, history, and age.	No exceptions noted.
03.01.02	Administrative access with the ability to change or modify client data are limited to authorized personnel based on job roles.	Inspected the administrative user listings to in-scope systems to determine whether access was restricted to authorized individuals based on job roles.	No exceptions noted.
03.01.03	Access to system resources is restricted from unauthorized users through the use of firewalls and secure connections.	Inspected the network diagram to determine whether external network access points had restrictions in place during the reporting period. Inspected the configuration settings to external firewalls to determine whether they were operational to restrict and protect the network's connection to the internet and prevent unauthorized traffic.	No exceptions noted.
03.01.04	The firewalls are configured to provide secure remote network access via a VPN tunnel to authenticate users with secure access.	Inspected the VPN configuration settings to determine whether secure tunnels were utilized for remote users accessing the network.	No exceptions noted.

DATASCAN

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests
Logical and Physical Access Controls		
Control Objective 03.02: Controls provide reasonable assurance that new internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.		
03.02.01 Approved new user access requests are initiated by the user's direct manager or the HR Department for new hires and contractors and are submitted to the IT Department via a change request.	For a sample of new hires and contractors, inspected access request approval documentation to determine whether new access to the system was completed and on file.	No exceptions noted.
03.02.02 Approved user access request change tickets resulting from an employee transfer or a change in a user's job role are initiated by the user's direct manager or the HR Department and are submitted to the IT Department via a change request. All network and system access levels are based on job roles.	Inspected the log of all employee transfers to determine whether any employee job transfers required modification of access during the testing period May 1, 2024 to October 31, 2024.	The operating effectiveness of this control could not be tested because the circumstances that warrant the operation of the control did not occur during the period.
03.02.03 Termination request tickets are initiated by the user's direct manager or the HR Department and are submitted to the IT Department via a change request to remove the user's access from the network and systems per company policy.	For a sample of terminated employees and contractors, inspected change request documentation to determine whether a change request ticket was on file and documented to remove system access per company policy.	No exceptions noted.
03.02.04 Client user accounts are created, modified, or removed based on authorized change requests sent by the customer to a designated client service representative.	For a sample of customer account changes, inspected customer account change documentation to determine whether a client authorization request was on file for each change.	No exceptions noted.
03.02.05 Roles are periodically reviewed and updated by management on an annual basis. Access change requests resulting from the review are submitted to the security group via a change request.	Inspected the annual user access review to determine whether user accounts and roles were reviewed by management on an annual basis.	No exceptions noted.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests
Logical and Physical Access Controls		
Control Objective 03.03: Controls provide reasonable assurance that physical access to the computer equipment, storage media, and documentation is only granted to authorized individuals.		
03.03.01 A physical access control system has been implemented at all entry and exit points of Datascan's corporate office. Additionally, visitors must be escorted by a Company employee when visiting areas where sensitive information or system components are maintained and operated.	Observed the visitor access processes in place to determine whether visitors must be escorted by an authorized employee when visiting Company facilities where sensitive information or system components were maintained and operated. Observed the access control system to determine whether the entry and exit points to the corporate office were secured and restricted to authorized personnel.	No exceptions noted.
03.03.02 Access lists to the data center are reviewed at least annually to verify the facility is restricted to authorized personnel. Change requests to the data center access list are initiated by the IT Department.	Inspected the annual access review of the data center access list to determine whether the facility was restricted to only authorized personnel and verified the list was reviewed annually.	No exceptions noted.
03.03.03 Management monitors the data center provider to ensure the controls at the data center which could affect the Company are operating effectively.	Inspected documentation to determine whether Management monitored the data center third-party service provider.	No exceptions noted.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests
Network and System Operations		
Control Objective 04.01: Controls provide reasonable assurance that the security of system components that could affect system integrity and processing errors with respect to user entities' internal control over financial reporting are monitored, evaluated, and countermeasures are implemented to resolve identified issues.		
04.01.01 Monitoring software is used on the critical systems to monitor system performance and availability and generates automatic alerts when certain protocols exceed thresholds relating to connectivity, processing capacity, and usage.	Inspected the system monitoring software configuration settings to determine whether key systems on the network were set to alert IT personnel when abnormal thresholds were reached.	No exceptions noted.
04.01.02 Antivirus software is installed on workstations, laptops, and servers with access to the external environment and is updated on a regular basis to protect against infection by computer viruses, malicious code, and unauthorized software.	Inspected the antivirus tool to determine whether the software was installed to prevent or detect the introduction of unauthorized or malicious software and scans were performed on a regular basis.	No exceptions noted.
Incident and Problem Management		
Control Objective 05.01: Controls provide reasonable assurance that application and system processing errors with respect to user entities' internal control over financial reporting are identified, tracked, recorded and resolved in a complete and accurate manner by authorized personnel.		
05.01.01 The Incident Management Policy describes the responsibilities and procedures of management and customers in the event of a system security breach or complaint and includes steps to be taken to coordinate the Company's response and remediation from such situations.	Inspected the Incident Management Policy to determine whether both internal and external users were provided with information on how to report incidents, concerns, and other complaints to authorized personnel.	No exceptions noted.
05.01.02 Operations personnel utilize issue tracking software for system support requests to identify, evaluate, report, and track issues or problems until resolution.	For a sample of issues, inspected the tickets to determine whether requests contained sufficient information to properly identify, evaluate, report, and resolve problems and issues throughout the problem management process.	No exceptions noted.
05.01.03 Technical reference documents are available to assist personnel in the resolution of common system processing errors and general troubleshooting.	Inspected the error resolution documents to determine whether they were available to personnel and contained systematic procedures to correct common processing errors that may occur in the IT environment.	No exceptions noted.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests
Change Management		
Control Objective 06.01: Controls provide reasonable assurance that the implementation of and changes to operating system software and data management systems with respect to user entities' internal control over financial reporting are authorized, tested, documented, approved, and implemented to result in complete and accurate processing and reporting of transactions.		
06.01.01 The Company policy describing the change management process defines the documentation and authorization of software and hardware changes to the system.	Inspected the Change Management Policy to determine whether defined processes were in place for software and hardware changes to the system.	No exceptions noted.
06.01.02 System change requests (i.e. infrastructure changes) not classified as minor are evaluated and approved to determine the potential effect of the change throughout the change management process.	For a sample of system changes, inspected change request ticket documentation to determine whether the change requests were reviewed and approved.	No exceptions noted.
06.01.03 Procedures are in place to document and track emergency changes and the changes are authorized and include a timely post implementation review in compliance with Company policy.	For a sample of emergency changes, inspected emergency change ticket documentation to determine whether the change requests were documented, authorized, and included a post implementation review.	No exceptions noted.
06.01.04 Procedures are in place for ensuring only reviewed and approved changes are made to production systems. These procedures include: • Documenting, testing, and authorizing code and database changes to the production environment prior to implementation • Separate test and production environments • Logical access procedures restrict the ability to migrate between development, test, and production environment to only authorized employees	For a sample of changes, inspected SDLC change tickets to determine whether the change/problem management ticketing system properly documented critical code changes to production, were authorized, and were tested prior to being implemented into production. Inspected the development, test, and production environments to determine whether the development and test environment was segregated from the production environment. Inspected the list of authorized users to determine whether only authorized employees had access to both the development and production environments.	No exceptions noted.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests
Data and System Backups		
Control Objective 07.01: Controls provide reasonable assurance that data and systems are backed up regularly and available for restoration in the event of processing errors or unexpected processing interruptions, with respect to user entities' internal control over financial reporting.		
07.01.01 All operationally critical components have redundant counterparts which are available to minimize downtime.	Inspected the architecture of redundant components within the Company's environment to determine whether redundant components were capable of providing the ability to continue operations in the event of a critical component failure.	No exceptions noted.
07.01.02 The Company uses a redundant strategy to backup uploaded client inventory data on a parallel SQL database via primary and secondary SQL servers with failover capabilities.	Inspected SQL server configurations to determine whether source files were processed on the primary and secondary SQL server.	No exceptions noted.
07.01.03 Client inventory data is retained in the system database for a minimum of 3 years.	Inspected date and time data in the Inventory Data Summary Report to determine whether inventory data was retained in an online database for three years.	No exceptions noted.
07.01.04 Client production data is backed up on at least a daily basis.	Inspected configuration settings to determine whether backups were configured to be performed on at least a daily basis.	No exceptions noted.
07.01.05 Backups are monitored via an automated system that sends notifications to alert IT personnel when backups are not successfully completed and the incident management process is initiated accordingly.	Inspected the backup configuration settings to determine whether automatic notifications were sent to IT personnel when backups were not successfully completed.	No exceptions noted.

Controls Specific by Contract Datascan, LP		Tests Performed by Baker Tilly	Results of Tests
Data Transmissions			
Control Objective 08.01: Controls provide reasonable assurance that data received with respect to user entities' internal control over financial is received from authorized sources and transmitted via secure methods.			
08.01.01	Transmission of confidential information beyond the boundary of the system occurs through the secured communication technologies to protect communications between authorized parties.	Inspected the configuration for system used to connect between internal and external users to determine whether it required secure communication methods to transmit data outside of system boundary.	No exceptions noted.
08.01.02	Inventory scanners are configured to transmit inventory data to the Company's system database via an encrypted connection.	Inspected the scanner configuration to determine whether inventory data transmissions sent from the inventory scanners was configured to be secured via encryption.	No exceptions noted.
Data Processing and Reporting			
Control Objective 09.01: Controls provide reasonable assurance that inventory data with respect to user entities' internal control over financial is processed and reported completely and accurately.			
09.01.01	The DART system does not allow inventory data to be uploaded into the system without completing the store setup process in order to verify all the required inventory setup information is completed before performing an inventory audit.	Observed an attempt to upload inventory data prior to completing the required inventory setup procedures to determine whether the DART system rejected the upload and notified the user of the errors.	No exceptions noted.
09.01.02	The DART system does not allow a store to close an inventory audit without an authorized user reviewing the system errors that resulted from the audit results and verifying all the system requirements for the inventory audit have been met prior to finalizing the inventory.	Observed an attempt to close an inventory audit before clearing all the failed error messages displayed in the audit results field to determine whether the DART system did not allow the inventory to be closed without resolving each error.	No exceptions noted.
09.01.03	Store fixture/zone tags are indexed with a sequential and unique number in order to provide identification and tracking of inventory assets.	Observed an attempt to enter fixture/zone tags with duplicate and non-sequential index numbers for a sample store to determine whether fixture/zone tags were automatically indexed with a unique and sequential number for tracking of inventory assets and that duplicate and non-sequential tags were rejected.	No exceptions noted.

Controls Specific by Contract Datascan, LP	Tests Performed by Baker Tilly	Results of Tests

Data Processing and Reporting

Control Objective 09.01: Controls provide reasonable assurance that inventory data with respect to user entities' internal control over financial is processed and reported completely and accurately.

09.01.04	Inventory data uploads are recorded in the DART system via transaction event logs that can be reviewed by authorized users for system analysis or troubleshooting if needed.	For a sample inventory upload, observed an upload of inventory data from a handheld inventory scanner to the DART system database to determine whether the system activities during the data upload process were recorded via transaction event logs that could be reviewed if needed.	No exceptions noted.
09.01.05	The DART system sends automatic email alerts to IT personnel when critical errors occur during the inventory data upload process in order to monitor issues and promote timely resolution.	Inspected DART system configurations to determine whether automatic email alerts were sent to IT personnel and confirm upload errors were flagged and logged.	No exceptions noted.
09.01.06	Inventory output files and reports are not generated before the inventory audit is closed in the DART system to ensure the inventory output files and reports sent to the client are accurate and complete.	For a sample of clients, inspected documentation to determine whether inventory output files and reports were not generated until the inventory audit had been closed in the DART system.	No exceptions noted.

Controls Specific by Contract Datascan, LP		Tests Performed by Baker Tilly	Results of Tests
Inventory Counts			
Control Objective 10.01: Controls provide reasonable assurance that store inventory count data is prepared and reported completely and accurately.			
10.01.01	The Datascan count team leader is responsible for understanding and agreeing to client policies and procedures through an acknowledgment for each count led.	For a sample of new team leads hired between May 1, 2024 and September 7, 2024, inspected written acknowledgments to determine whether team leads understood and agreed to client policies and procedures. Inspected system configurations after September 7, 2024 to determine whether DART is configured to restrict the ability to close an audit prior to acknowledgment of adherence to client policies and procedures from the team lead.	No exceptions noted.
10.01.02	Access to make adjustments, review amounts, and close an audit is restricted to authorized personnel.	For a sample of users with access to the DART counting web portal, inspected job titles to determine whether access was restricted to authorized personnel.	No exceptions noted.
10.01.03	Inventory count adjustment reports are reviewed and approved according to the account policies and procedures as agreed to in the contract between Datascan and the applicable customer.	For a sample of counts, inspected inventory count adjustment reports to determine whether they were reviewed in accordance with the contract between Datascan and the applicable customer.	No exceptions noted.

Controls Specific by Contract Datascan, LP		Tests Performed by Baker Tilly	Results of Tests
Inventory Counts			
Control Objective 10.01: Controls provide reasonable assurance that store inventory count data is prepared and reported completely and accurately.			
10.01.04	The DART system restricts the ability to close an audit prior to completion of all tasks assigned for the store audit.	Inspected system configurations to determine whether DART was configured to restrict the ability to close an audit prior to the completion of all tasks assigned for the store audit.	No exceptions noted.
10.01.05	Prior to the close of an inventory count, any count adjustments made must have a rationale associated with the adjustment, as required by the customer.	For a sample of counts, observed the count process to determine whether all variances identified by the client were investigated by validating the original amount for accuracy and any errors identified were resolved.	No exceptions noted.
10.01.06	Every area tag must be accounted for before an inventory count can be closed.	Observed an attempt to close an inventory audit before every area tag is closed to determine whether users were systematically restricted from closing an audit before every area tag is closed.	No exceptions noted.
10.01.07	Inventory items are counted in accordance with client policies and procedures	Inspected policies and procedures to determine whether count procedures have been established. For a sample of counts, observed the count process to determine whether the count was performed in accordance with policies and procedures.	No exceptions noted.
10.01.08	Area tickets are placed in accordance with client policies and procedures.	Inspected policies and procedures to determine whether area tickets placement procedures have been established. For a sample of counts, observed the count process to determine whether area tickets were placed in accordance with policies and procedures.	No exceptions noted.
10.01.09	Data received is systematically validated to ensure that data is complete and accurate. Issues are investigated and remediated.	Inspected data transmission specifications to determine whether data transmissions from clients were systematically validated for completeness and accuracy.	No exceptions noted.

Controls Specific by Contract Datascan, LP		Tests Performed by Baker Tilly	Results of Tests
Inventory Counts Personnel			
Control Objective 10.02: Controls provide reasonable assurance that personnel participating in full service counts have backgrounds verified and are trained for competence.			
10.02.01	Background checks are performed prior to onboarding for employees and contractors that perform full-service count services.	For a sample of new employees and contractors, inspected logs to determine whether new employees and contractors have their background checked prior to onboarding.	No exceptions noted.
10.02.02	All new employees and contractors that perform full-service counts are required to take training for proper performance of counting procedures.	For a sample of new full-service count employees and contractors, inspected evidence to show that counting training was received. Inspected system configurations to determine whether DART is configured to restrict the ability to close an audit prior to acknowledgment of count performance by trained employees and contractors.	No exceptions noted.
10.02.03	The Datascan count team leader is responsible for understanding and agreeing to client policies and procedures through acknowledgment for each count led.	For a sample of new team leads hired between May 1, 2024 and September 7, 2024, inspected written acknowledgments to determine whether team leads understood and agreed to client policies and procedures. Inspected system configurations after September 7, 2024 to determine whether DART is configured to restrict the ability to close an audit prior to acknowledgment of adherence to client policies and procedures from the team lead.	No exceptions noted.