

DCL, Inc. (formerly known as DisCopyLabs)

- Manufacturing and Logistics Services

SAS No. 70 Report on Controls Placed in Operation

As of March 31, 2006 and Tests of Operating Effectiveness for the  
Period of October 1, 2005 – March 31, 2006



DCL, Inc.

**Report on Controls Placed in Operation and Tests of Operating Effectiveness for DCL, Inc.’s  
Manufacturing and Logistics Service**

**Table of Contents**

---

	<u>Page</u>
Section I - Independent Service Auditor’s Report .....	3
Section II – Service Organization’s Description of Controls .....	5
A. Scope and Purpose of the Report.....	5
B. Overview of Operations.....	5
C. Control Environment .....	7
D. Risk Assessment .....	9
E. Monitoring.....	9
F. Information and Communication.....	9
G. User Control Considerations.....	13
H. Glossary/Acronyms.....	14
Section III - Information Provided by the Service Auditor.....	15

## I. Independent Service Auditor's Report

To the Board of Directors of DCL, Inc.:

We have examined the accompanying description of the controls for DCL, Inc. ("DCL") as it relates to DCL's Manufacturing and Logistics Service. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of DCL's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied the internal controls contemplated in the design of DCL's controls; and (3) such controls had been placed in operation as of March 31, 2006. The accompanying description includes only those control objectives and related controls at DCL and does not include controls and related control objectives of external organizations. The control objectives were specified by the management of DCL. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the controls at DCL presents fairly, in all material respects, the relevant aspects of DCL's controls that had been placed in operation as of March 31, 2006. Also, in our opinion, the controls as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the user organizations applied the controls contemplated in the design of DCL's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls to obtain evidence about the effectiveness in meeting the related controls objectives during the period from October 1, 2005 to March 31, 2006. The specific controls, related control objectives, and the nature, timing, extent and results of the tests are summarized on pages 15 through 29 of this report. This information has been provided to the user organizations of DCL and to their auditors to be taken into consideration, along with information about the internal controls at user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested, as described on pages 15 through 29, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives specified on those pages were achieved during the period from October 1, 2005 to March 31, 2006.

The relative effectiveness and significance of specific controls at DCL, and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at DCL is as of March 31, 2006 and information about tests of operating effectiveness of specific controls covers the period from October 1, 2005 to March 31, 2006. Any projection of such information to the future is subject to risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at DCL is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system of controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the Board of Directors and Management of DCL, its users, and the independent auditors of its users.

GRANT THORNTON LLP

*Grant Thornton LLP*

San Jose, California  
April 6, 2006

## II. Service Organization's Description of Controls

### A. Scope and Purpose of the Report

This report describes the control structure of DCL, as it relates to DCL's Manufacturing and Logistics Service as of March 31, 2006 and includes tests of operating effectiveness for the period from October 1, 2005 to March 31, 2006.

The report was prepared according to the guidance contained in American Institute of Certified Public Accountants ("AICPA") Statement on Auditing Standards No. 70, "Reports on the Processing of Transactions by Service Organizations" ("SAS 70") as amended by AICPA Statement on Auditing Standards No. 78, "Consideration of Internal Control in a Financial Statement Audit" ("SAS 78") and AICPA Statement on Auditing Standards No. 88, "Service Organizations and Reporting on Consistency" ("SAS 88"). The amendments in SAS 78 recognize and incorporate the definition and description of internal control as contained in "Internal Control – Integrated Framework," published by the Committee of Sponsoring Organizations of the Treadway Commission. The amendments in SAS 88 clarifies that the SAS is applicable if an entity obtains services from another organization that are part of the entity's information system and provides guidance to determine whether services are part of the information system and clarifies the factors that should be considered in such determination. As this report is intended to respond to SAS 70, it does not encompass all aspects of the services provided or procedures followed by DCL.

### B. Overview of Operations

#### 1. Company Overview

DCL, formerly known as DisCopyLabs, is a leading provider of outsourced manufacturing and logistics services for technology industries. Founded in 1982, DCL is headquartered in Fremont, California. Its customers include hardware and medical device manufacturers, and software publishers. DCL's business-to-business and business-to-consumer services include turnkey manufacturing, packaging and assembly, fulfillment and distribution, warehousing and returns management.

#### **DCL Mission**

*DCL earns long term partnerships with its customers by providing quality, turnkey manufacturing and distribution services that are competitively priced and delivered on-time.*

## 2. Services Provided

With over 300,000 square feet under roof, DCL is located in Northern (Fremont) and Southern (Ontario) California, providing turnkey manufacturing services complemented by warehousing, inventory management, purchasing, materials management, fulfillment, freight management and reverse logistics.

- **Material Management:** Utilizing ERP (Enterprise Resource Planning) tools, DCL projects the appropriate inventory levels necessary to comply with customers' requirements. Inventory levels are set to prevent loss of investment dollars stemming from obsolescence or extended storage of inventory. Purchasing decisions factor both economic reorder quantities and lead times.
- **Fulfillment and Freight Management:** DCL has capabilities to pick, pack and ship over 15,000 separate orders per day. Utilizing bar codes, DCL provides for 100% verification of the products picked and packed; printed appropriate carrier manifest labels, associated packing lists, bills of lading, and international documents.
- **Assembly:** DCL has the capability to assemble and package over 200,000 products per day. With over 10 assembly lines -- manual, semi-automated or automated -- by running multiple shifts, DCL can assemble a variety of packages to meet seasonal or new product launch programs of its customers.
- **Warehousing:** DCL has over 12,000 pallet locations to support assembly and fulfillment requirements. Its warehouse management system administers the kit process and cycle count programs for DCL in order to maintain needed inventory accuracies.
- **Reverse logistics:** DCL provides returns management to identify product returns for appropriate credit or exchange. DCL sorts products for damage and returns for credit, retail stock exchange, or return to vendor.
- **Specialized requirements:** DCL provides e-commerce solutions, from storefronts to accessing inventory, work in process and shipping information. DCL handles the secured printing and tracking of digital rights licenses or enabling certificates. DCL interfaces include EDI 810, 850, 852, 855, 856, and 860 documents and other electronic exchanges.

DCL has been ISO-certified since 1994 and is currently at ISO 9001:2001. DCL utilizes the two locations as a business continuity solution. The DCL database, which includes specifications and requirements, is backed up weekly and stored off site. In case of an emergency, where one location cannot operate, the other location accesses the back up database, with all the necessary specifications and requirements, to provide business continuation for the clients.

## C. Control Environment

### 1. Management and Organization

DCL is departmentalized with directors or above reporting directly to the President. Directors are responsible for the oversight of company activities as related to their respective departments. The President defines and executes business strategy and oversees operations in compliance with its Bylaws and Board of Directors' recommendations.

Incorporated in the State of California in 1982 and operating in good standing, DCL has seven Board members who meet quarterly to review the company performance and provide oversight of the President on strategy, policies and compliance to the laws and bylaws governing the company. The Chairman of the Board is the principal stockholder of the company and as CEO, is responsible for marketing and sales. The President is a member of the Board of Directors and holds substantial shares in the company. Three of the Directors' seats are held by individuals who have no day to day responsibilities in the company. These are individuals who are well established in the business community and have essential experience with other businesses, serving either on their boards or in executive positions for start up or publicly held companies.

#### **Board of Directors**

**Denis Coleman**, Executive Chairman of Solus Biosystems, a startup in biotech tools, was instrumental in the formation of DCL. As the designer of the first spelling check program for personal computers, Denis inspired Norman and David Tu to create a manufacturing service to support software publishers. Denis has since founded or co-founded breakthrough technology companies including Symantec Corporation, Visioneer Communications, C Level Design Corporation and Claria Corporation. With a Ph.D. in management and computer systems from Stanford University and undergraduate and graduate degrees from MIT, Denis taught at Stanford, University of Hawaii and York University in Canada.

**Chris Paisley**, Dean's Executive Professor of Accounting and Finance at the Leavey School of Business at Santa Clara University, has served on DCL's Board for over 20 years. Retired as Senior Vice President of Finance and Chief Financial Officer for 3Com Corporation, Chris was also involved in finance at Ridge Computers and Hewlett Packard. He serves on the Board of Directors for numerous Silicon Valley companies including Volterra, Electronics for Imaging, and Brocade Communications Systems. Chris earned an MBA from UCLA and a B.A. degree from UC Santa Barbara.

**Tom Hubbs**, Executive Vice President and Chief Financial Officer of Bytemobile, Inc., has been involved in financial management for 35 years for numerous technology and business companies. Tom successfully launched initial public offerings and mergers for such companies as interWAVE Communications International, Ltd., VeriFone, Inc. and Ungermann-Bass, Inc. On the Board of Directors for three technology industry companies, Tom holds an MBA from Santa Clara University and a B.S. degree from Lehigh University in Pennsylvania.

#### **Management**

##### **Norman Tu**, *Chairman and CEO*

Norman is active in business development, marketing and finance activities at DCL. Since 1982, Norman has focused on strategically positioning DCL as the market leader for outsourced supply chain solutions. His vision resulted in the creation of *eFactory*, the industry's first online, web-based reporting tool. Prior to co-founding DCL in 1982, Norman was a systems analyst and technical manager at Hewlett

Packard for nine years. He was a field systems engineer at Xerox Data Systems from 1969 to 1973. Norman received a B.S. degree in Computer Science from Chico State University.

**David Tu, *President***

David, a co-founder of DCL, directs DCL's operations and business planning systems. He is instrumental in transforming DCL into a supply chain management service that uses cutting edge technology to support manufacturing operations and customer needs. He initiated ISO procedures, earning DCL's first ISO 9002 certification in 1984 and DCL's recent ISO 9000:2001 recertification. David served as an operations consultant to DCL prior to joining DCL full-time in 1988. Previously, David was Vice President for The Shorenstein Company from 1983 to 1988. David holds B.S. and Master in Engineering degrees in civil engineering from the University of California Davis and an MBA degree from Golden Gate University.

**Shahid Massod, *Vice President, IT and e-Commerce***

Shahid applies more than 20 years of diverse experience in computers, control systems, manufacturing, retail and distribution towards developing systems and processes using state-of-the-art technologies that meet the needs of DCL's clients and organization. Prior to joining the Company in 1995, Shahid held positions with Honeywell, Lear Siegler, Valmet Automation, Sentrol Systems, Compucenter and Access Business Systems. Shahid received his B.S. degree in Electrical Engineering from California Polytechnic University and an MBA from York University.

**Scott Daub, *Director, Operations – Northern California***

Scott directs the production and manufacturing operations of DCL's Fremont facilities. Prior to joining DCL in 2002, Scott spent 12 years with Symantec in various operation management capacities. Scott obtained a B.S. degree in Commerce from Santa Clara University.

**Larry Shaker, *Director, Operations – Southern California***

Larry manages the manufacturing and business operations of DCL's Ontario facility. Larry joined DCL in 1997 as the Operations Manager for Southern California. Prior to joining DCL, Larry had over 25 years in manufacturing, including 18 years with Owens Illinois in various manufacturing management capacities. Larry holds a B.A. degree in Business Administration from California State University at Fullerton.

**Mary Kung, *Director, Strategic Accounts***

Mary directs all manufacturing and distribution requirements for DCL's strategic customers. Prior to joining DCL in 1985, Mary was a manager for Read & Emerick, a multi-national trading company in New York. Mary graduated from Hong Kong Baptist College with a B.A. degree in Business Administration.

## **2. Personnel Policies**

DCL's hiring practices ensure that new employees are qualified for their job responsibilities. Hiring practices include minimum requirements for education and experience commensurate with the position, background checks, confidentiality statements, and the company's Policies and Procedures acknowledgment. Job descriptions are documented and posted on the company portal.

Human Resources (HR) is responsible for training and development so that all personnel have the opportunity to cultivate and refine skills related to their functional responsibilities. Safety and security training are given continuously in order for personnel to perform their responsibilities in a safe and secure manner. For selected responsibilities, in particular IT and those responsible for digital rights

licenses and financials, background checks are performed quarterly. HR monitors and maintains the issuance of passwords to key applications to assure that the personnel job responsibilities are consistent with the rights granted by the password. To monitor the proficiency of its employees, formal performance reviews are conducted annually.

## **D. RISK ASSESSMENT**

Annually, as part of DCL's process improvement review, DCL identifies those risks that could potentially affect DCL's capability to provide service within the risk tolerances of its customers. The risk assessment process consists of, but is not limited to:

- Evaluating the production, fulfillment and storage capacity in comparison to the projected demands;
- IT infrastructure for redundancy and data integrity to maintain a consistent and accurate exchange of data;
  - Security practice and infrastructure to prevent improper access to and manipulation of data;
  - Business continuity process to assure the timely access of critical information by the supporting site in the event of a site shut down due to events out of its control;
- Security practice and monitoring to ensure proper containment and processing of physical products and digital rights licenses;
- Inventory management to ensure the proper accounting of customers' material or products which materially affects the customers' financial status.

The risk assessment process is designed to help ensure that the correct controls or actions have been implemented to mitigate the identified risks.

## **E. MONITORING**

At least once per year, management personnel meet with key customers whose requirements impact the capacity of production, fulfillment and/or storage. Based on the projections, management determines if capacity needs to be added or reduced and, if appropriate, changes to systems and processes are needed to increase efficiencies, and by definition increase capacity. Additionally, management reviews the percentage use of capacity by quarter. By the nature of its customers, which have substantial peak load demands, the ongoing use of capacity must be well below the available capacity. Capacity extensions are executed by adding additional shifts of operations including running 24 hours, weekends and holidays. Expansions of warehouse and production facilities are long term commitments and are made in concert with the primary customers.

## **F. INFORMATION AND COMMUNICATION**

### **Information Systems Environment**

DCL utilizes a Windows 2003 based platform environment with Active Directory. The network is secured by multiple firewalls which includes intrusion detection capabilities. There are a total of 60-70 workstations at each location in Fremont and Ontario. Active Directory domain policies are used for

network authentication and adhere to Microsoft's Standard Best Practice Policy. Remote access is granted through VPN client control along with password and active directory registration.

Primary servers at each location are blade servers with SAN storage providing for failover redundancy capabilities to ensure downtime is minimized and within the tolerances established with its customers. Servers are connected by dual T1 (diverse) line for redundancy with additional VPN available for additional redundancy. IT administration procedures are documented to include all daily procedures that are to be performed by the system administrator. Daily incremented backups are run with full back up performed weekly. The weekly backup is picked up and stored by an outside archiving service.

Servers are supported by UPS power source providing for 30 minutes of power. The primary server farms at Fremont and Ontario are connected to natural gas back up generators which provide continuous power prior to the demise of the UPS power source.

### **Enterprise Resource Planning Application**

DCL's primary tool for planning, inventory management and production control is application produced by Oracle (formerly JD Edwards One World). The host application interfaces with an application server that is connected to a SQL 2003 database. The system is secured by authenticating the users via Active Directory prior to granting access. Data is processed and viewed by authorized users of DCL in a "real time" mode.

Transactions are executed through manual or transaction devices or interface to other transaction processes. All access points for transaction are controlled through the Active Directory and password. Oracle maintains transaction histories for auditing and reconciliation purposes.

### **Information Technology Application Procedures**

#### Logical Security and Monitoring

DCL users are required to have valid user-ID's and passwords to access the company network and applications, both at the office or remotely. Each user ID does restrict system privileges based on job duties and responsibilities. Each employee is responsible for his/her user ID and password. User passwords are set to allow no less than a minimum number of characters and expire on a scheduled basis. Additionally, an attempt to login using the incorrect password more than a certain number of attempts will lock the user out of the system until the password is reset manually by the System Administrator.

Access is granted to an employee per a specific request from the employee's manager to Human Resources. HR reviews the request for consistency with the employee's job description and, if approved, coordinates with IT System Administrator to grant the appropriate level of access. Remote access is available through VPN tunnel, authenticating to a Remote Access Server. Documented procedures are in place for logical access including new user setup requirements, job change and employee termination procedures.

System Administrator monitors the performance of the servers and the firewall to assess incompatible activities. Exceptions to the standard performance are reported to the VP IT on a scheduled basis for additional follow up or remedies. Based on the criticality of the exception, the reporter seeks immediate escalation. Document procedures are in place for the review of activities of the firewall and other system administration and network activities.

The server supporting the management and printing of digital management licenses is a stand alone network and resides in a secured room. All I/O ports, other than those connected to the printers and workstations, are disabled.

#### Change Control- Systems/Application

The Oracle ERP application is the primary application used by DCL for planning, inventory control, and production processing. The ERP application is a third party vendor, Oracle, which releases periodic updates to enhance features or resolve application issues. DCL's internal IT resources utilize the tool sets available through Oracle, customizing the "look and feel" screens to align with DCL's workflow and process.

The Vice President of IT manages all updates and customizations and approves all IT requirements submitted either internally or by customers. The VP IT determines the timeframe and the test process for implementing approved submissions. He takes the lead role in defining the final scope with either the customer or internal management and in assessing the impact on the system and/or the organization. He coordinates the execution of the scope through consultants or internal staff. Documented procedures are in place for Change Control and environmental changes. The VP IT directs the testing of the development in the test environment and identifies and resolves issues prior to introducing the development into the production environment. Testing feedback and development documentation are tracked with revision tracking logs to identify the changes and time. The VP IT is the approving authority for movement of the development from testing to the production environment. The System Administrator, acting with executive approval, coordinates with Operations to determine the appropriate schedule for the movement to production environment.

#### Building and Data Center Physical Security

DCL facilities are secured by card access with only authorized individuals having access. Human Resources manage the authorization of the card access and grants the rights of access based on the employees' responsibilities. All active egress points are monitored by digital cameras which the images are maintained for a 30 day period. All non-active egress points have local alarms which activate when the egress is opened. During off-hours all egress points have contact alarms and infra-red beams which scan open areas for motions. Activation of the either the contact points or motion detectors are monitored by a third party service and reported to the local police.

All visitors are required to register in the main lobby with the Receptionist. The Receptionist verifies with the appropriate manager or staff personnel that the visitor(s) have a valid appointment. Each visitor is required to sign a non-disclosure acknowledgement prior to granting entrance to the facility. All visitors are escorted while in the facility.

Human Resources provide safety and security members to monitor the employees' entrance. They coordinate with the contract staff service to identify staff contracted to work for the requirements of the day.

Warehouse and Distribution supervisory staff keep all access closed if there are no activities. If the dock doors are open to provide air flow for temperature control of the warehouse and production area, the opening must be secured by a locked gate. Any time an access is open, a DCL employee or contract staff must be within the vicinity monitoring the activities. If a driver requires access to the facility, the supervisor of the affected entrance, shipping or receiving, will arrange for an escort.

IT servers and the digital rights license printing areas are designated as critical and access further control by biometric locks. Critical area access is granted through Human Resources. Those individuals must agree to scheduled background checks for the continual rights to access these areas. Key areas of the server room and the digital right license printing areas are monitored by digital cameras. Primary server rooms are monitored for temperature limits by a third party monitoring service. The digital rights license printing is further secured with a wire mesh ceiling, steel door and high impact plastic windows.

All facilities are constructed to comply with the appropriate building codes and are fully sprinklered. Monitoring of the sprinklers, smoke and motion detectors are performed by a third party service. Depending on the incident, the third party service will either contact the police or contact the assigned employees.

## **Operation Controls**

### **Procurement**

Price and quantities of purchases of components are approved either directly or through guidelines previously agreed to by the customers. For those customers who provide perpetual forecasts, DCL utilizes the planning application in Oracle to extract the necessary purchases in relation to existing inventories and the forecasts. Business rules are in place to define the time window which DCL maintains the inventory in support of the forecasts. The financial responsibility of these components is DCL's until the components are assembled into finish goods.

Purchase orders issued by the customers provide DCL the approval to issue work orders to assemble the components into the finish goods. Upon completion of the work orders, DCL makes the appropriate transactions in Oracle for the finished goods and makes the associated deductions of components. Additional, DCL notifies the customers of the finished goods inventory either by email or by transacting in the appropriate customer's system to close the purchase orders. The finished goods transaction identifies the products as customer-owned and available for fulfillment or distribution orders from the customer. Daily cycle counts maintain the accuracy of finished goods inventories. Periodically, customers perform their own cycle counts to validate DCL's inventory positions.

### **Order Fulfillment**

Fulfillment or distribution orders to ship customer's inventory are primarily provided to DCL electronically. Throughout the day, customers process orders and place batches of those orders into a secure ftp site. DCL polls these sites, locates the batches and pulls them into the DCL order process front end. As part of the front end process, orders are checked for required fields. An acknowledgement email is sent to a designated group or individual, summarizing the orders that have been successfully processed into DCL's system and identifying those orders requiring corrections.

Periodically throughout the day, a return file is generated containing the order information, such as the tracking number, carrier, weight and products shipped. The return file is posted onto the customers' secured ftp site for processing on their part. Depending on the customers, either an accumulative or incremental file is sent. Resolutions of discrepancies recreate the return file, to incorporate the missing orders or details of the orders, are sent to the customer for their manual transaction.

Continuously throughout the day, the Fulfillment Manager or supervisors reviews the backlog and monitors priorities to ensure that expedited orders or orders from the previous day are handled in a timely manner.

### **Obsolete transactions**

Instructions to cancel, modify or discard customer owned components or finish goods are provided to DCL through written instructions. Acknowledgements via email are provided to customers upon completion of discarding of the material requested.

### **Inventory Management Controls**

Fulfillment transactions are provided to the customers multiple times each day of operations. These transaction files acknowledge that finished goods or components were shipped in accordance to instructions provided by customer. DCL notifies customers if any of the finished goods or components failed to leave the facility, as represented by the acknowledgement file.

Customers, at times, perform independent cycle counts to confirm their inventory quantities. DCL coordinates inventory movement and resources to support the reconciliation of the inventory and transactions.

### **G. User Control Considerations**

The successful implementation of the production and fulfillment of customers' requirements is only achieved with comprehensive controls on the part of both DCL and its customers. Each customer evaluates its internal control structure to determine if the appropriate controls are in place. Listed below is a partial list of controls which address only those controls surrounding the interface and communication between the customer and DCL.

- Fulfillment or distribution orders provided by customers will be accurate and compliant with laws or legal statutes associated with the products.
- Customer represents that materials provided to DCL are legally owned or properly licensed by the customer.
- DCL will rely upon the written instructions of individuals authorized to interface with DCL. Written instructions are commonly provided to DCL in email.
  - Customer is responsible for notifying DCL of changes to its authorized personnel.
- Customer is responsible for providing the value and trade compliant information necessary for the legal export of their products.
- Customer is responsible for the proper interface of data provided by DCL.
  - Customer is responsible for any manual transactions due to errors or omissions.
- For customers where DCL forwards receiving documents to the customer, the customers are responsible for reviewing the documents and recording the receipt based upon the receipt date on the document.
- For customers providing DCL an access to the former's application, customer should only grant DCL personnel access to close Purchase Orders and deny the ability to create/modify Purchase Orders.

## H. Glossary / Acronyms

1. SAN – Storage Area Network support disk mirroring, backup and restore, archival and retrieval of archived data, data migration from one storage device to another and the sharing of data among different servers in a network.
2. VPN - A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one.
3. T1 - A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires. T1 lines are used for heavy telephone traffic, or for computer networks linked directly to the Internet. T1 lines are normally used by small and medium-sized companies with heavy network traffic. They can send and receive very large text files, graphics, sounds, and databases very quickly
4. SQL (Structured Query Language) - SQL database is a type of database technology that is the most widely used in today's computing environment. Here the data is stored in a very structured format that provides high levels of functionality. SQL databases are generally more robust, secure and have better performance than other older database technologies.
5. ERP (Enterprise Resource Planning) - software that integrates departments and functions across a company into one computer system. ERP runs off a single database, enabling various departments to share information and communicate with each other. ERP systems comprise function-specific modules designed to interact with the other modules, e.g. Accounts Receivable, Accounts Payable, Purchasing, etc.

### III. Information Provided by the Service Auditors

This section presents the following information provided by DCL:

- The control objectives specified by the management of DCL.
- The controls established and specified by DCL to achieve the specified control objectives.

Also, included in this section is the following information:

- A description of the testing performed by the service auditors to determine whether specific controls, identified by DCL, were operating with sufficient effectiveness to achieve specified control objectives. The service auditors determined the nature, timing, and extent of the testing performed.
- The results of the service auditors' tests of operating effectiveness.

Tests performed of the operational effectiveness of the controls detailed in the following matrices are described below:

<b><u>TYPE</u></b>	<b><u>DESCRIPTION</u></b>
<b>Inquiry</b>	<p>Inquired of appropriate personnel. Inquires seeking relevant information or representation from DCL personnel were performed to obtain among other things:</p> <ul style="list-style-type: none"> <li>▪ Knowledge and additional information regarding the policy or procedure.</li> <li>▪ Corroborating evidence of the policy or procedure.</li> </ul> <p>As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the accompanying matrices.</p>
<b>Inspection</b>	<p>Inspected documents and records indicating performance of the controls. This includes among other things:</p> <ul style="list-style-type: none"> <li>▪ Inspection of reconciliations and management reports that age or quantify reconciling items to assess whether balances and reconciling items are properly monitored, controlled and resolved on a timely basis.</li> <li>▪ Examinations of source documentation and authorizations to verify propriety of transactions processed.</li> <li>▪ Examination of documents or records for evidence of performance, such as existence of initials or signatures.</li> <li>▪ Inspection of DCL systems documentation, such as operations manuals, flow charts and job descriptions.</li> </ul>
<b>Observation</b>	Observed the application or existence of specific controls as represented.

**Control Objective No. 1**

**Controls activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of its personnel.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. Organizational policy statements and codes of conduct are documented.	<b>1. Inspection:</b> Obtained and reviewed the latest copy of the DCL Employee Handbook and verified that the Handbook included an organizational Introductory Statement and sections on Harassment, Workplace Violence, Internal Investigations and Non-Disclosure of confidential information.	No Relevant Exceptions Noted
2. Employees sign forms acknowledging their acceptance of the Employee Handbook and Confidentiality addendum. By doing so, the employee agrees to abide to the Organizational policies.  Temporary workers or contractors sign Non-Disclosure agreements.	<b>2. Inspection:</b> Inspected and reviewed judgmental samples of employee files to ensure that a signed copy of the acknowledgement form to the Handbook and Confidentiality addendum was available.  Inspected and reviewed a judgment sample of temporary workers or contractor files to ensure that a signed copy of the Contractor Non-Disclosure Agreement is available.	No Relevant Exceptions Noted
3. Updates to the Employee Handbook are performed in a controlled fashion that includes approvals and version controls.	<b>3a. Inquiry:</b> Inquired of the HR Manager and determined that HR maintains version control of the Employee Handbook.	No Relevant Exceptions Noted
	<b>3b. Inspection:</b> Inspected the Employee handbook to determine if it is dated for version control purposes.	No Relevant Exceptions Noted
4. Background checks are performed for employees and contractors involved in sensitive functions.	<b>4a. Inquiry:</b> Inquired of the HR Manager to determine that background checks are performed for employees and contractors involved in sensitive functions.	No Relevant Exceptions Noted
	<b>4b. Inspection:</b> Inspected a judgmental sample of employee files to ensure background forms were complete and available. Reviewed the HR Background Check Report that identifies the date of the last background check for the sampled employees and certain contractors with access to sensitive information.	No Relevant Exceptions Noted
5. Management has considered the competence levels of particular job positions and has documented required skills, responsibilities, and knowledge levels in the form of written position requirements.	<b>5. Inspection:</b> Inspected a judgmental sample of current written job descriptions to determine that management had considered the competence levels for particular job positions and had documented required skills, responsibilities, and knowledge levels in the form of written position requirements.	No Relevant Exceptions Noted

6. Management performs annual employee reviews.	<b>6. Inspection:</b> Inspected a judgmental sample of employee files to ensure annual performance review forms were complete and available.	No Relevant Exceptions Noted
7. Management meetings are held on an ongoing basis to discuss operational issues.	<b>7. Inspection:</b> Inspected a judgmental sample of quarterly update meeting agendas/minutes to determine that management meetings were held on a quarterly basis to discuss operational issues.	No Relevant Exceptions Noted
8. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated on an as-needed basis.	<b>8a. Inquiry:</b> Inquired of the HR Manager to determine that the organizational chart is online to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No Relevant Exceptions Noted
	<b>8b. Inspection:</b> We inspected the organization chart (WP 1.8a and 1.8b) and found that it reflects the current organization. If updates are required, the organization chart is updated by HR and posted on the internal website.	No Relevant Exceptions Noted
9. Insurance policies are in place to mitigate the risk of certain business interruptions.	<b>9a. Inquiry:</b> Inquired of the HR Manager to determine that insurance policies are in place to mitigate the risk of certain business interruptions.	No Relevant Exceptions Noted
	<b>9b. Inspection:</b> Inspected insurance documentation and determine insurance coverage for Commercial General Liability (w/c includes errors and omission), Automobile Liability, Excess Liability, Workers Comp & Fiduciary Insurance.	No Relevant Exceptions Noted
<b>Conclusion: Observed the application or existence of specific controls as represented.</b>		

**Control Objective No. 2**

**Control activities provide reasonable assurance that access to and movement within the DCL facilities are properly controlled and monitored. Additionally, access to server rooms, storage media, and other critical infrastructure is limited based on job responsibilities.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. Staff access to the Server room, Master Room, and DRM room is reviewed on a semi-annual basis.	<b>1. Inspection and Inquiry:</b> Inspected HR Security Access Report and performed inquiries with the HR Manager to determine that access is reviewed.	No Relevant Exceptions Noted
2. The Server Room and Master Room have a key lock or a biometric device.	<b>2. Observation:</b> Observed the Server Room and Master Room to determine whether a key lock or a biometric device is in place.	No Relevant Exceptions Noted
3. A limited number of personnel have access to the Server Room. Access is restricted based on job responsibility.	<b>3a. Inspection:</b> Inspected the server room access list to determine that access to the Server Room is limited. Further reviewed the terminated employee list to ensure access was not available to terminated staff.	No relevant Exceptions Noted
	<b>3b. Inquiry:</b> Inquired of the HR Manager as to the business reason for the access of employees indicated in the access list.	No Relevant Exceptions Noted
4. The Server Room is monitored with the use of video cameras and alarms.	<b>4. Observation:</b> Observed the presence of video cameras and alarms in the server room.	No Relevant Exceptions Noted

**Conclusion: Observed the application or existence of specific controls as represented.**

**Control Objective No. 3**

**Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. The Server Room is protected by fire detection and suppression controls that include fire alarms, fire suppression equipment, fire detectors and hand-held fire extinguishers.	<b>1. Observation:</b> Observed the server room facility to determine that it was protected by fire detection and suppression controls that include fire alarms, fire suppression equipment, fire detectors and hand-held fire extinguishers.	No Relevant Exceptions Noted
2. The server room is equipped with dedicated air conditioning units and a thermostat. The air conditioning systems are inspected and maintained to ensure they are functioning as expected.	<b>2a. Observation:</b> Observed the server room facility to determine that it was equipped with a dedicated air conditioning unit.	No Relevant Exceptions Noted
	<b>2b. Inspection:</b> Inspected the air conditioning maintenance documentation to determine that they were inspected and maintained to ensure that they were functioning as expected.	No Relevant Exceptions Noted
3. The server room is connected to a UPS system. Electricity is stored by the UPS system and the system can provide temporary electricity in the event of a power outage. The UPS also mitigates the risk of power surges impacting infrastructure in the server room.	<b>3. Observation:</b> Observed the UPS system to determine that the server is connected to a UPS system.	No Relevant Exceptions Noted
4. Fire and alarm systems are inspected to verify compliance with fire regulations.	<b>4. Inspection:</b> Inspected the fire and alarm inspections to determine that the third party specialists verified compliance with fire regulations.	No Relevant Exceptions Noted
5. Fire extinguisher systems are inspected to verify compliance with fire regulations.	<b>5. Inspection:</b> Inspected the fire extinguisher systems to determine that the fire extinguisher systems were inspected to verify compliance with fire regulations.	No Relevant Exceptions Noted
6. The fire suppression system is inspected and maintained to ensure they are functioning as expected.	<b>6. Inspection:</b> Inspected maintenance report for the fire suppression system to determine that the system was inspected and maintained to ensure it was functioning as expected.	No Relevant Exceptions Noted

**Conclusion: Observed the application or existence of specific controls as represented.**

**Control Objective No. 4**

**Control activities provide reasonable assurance that timely system backups occur and backup tapes are rotated and stored off-site.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. Formal system backup procedures are in place for critical system.	<b>1. Inspection:</b> Inspected System Back-Up procedures to determine formal work instructions were in place.	No Relevant Exception Noted
2. An automated system is utilized to perform system backups.	<b>2a. Inquiry:</b> Inquired of the operations team to determine that automated systems were utilized to perform system backups.	No Relevant Exception Noted
	<b>2b. Observation:</b> Observed backup system configurations to determine that automated systems were configured to backup of critical data.	No Relevant Exceptions Noted
3. Data backup files are stored in a secure location and rotated offsite.	<b>3a. Observation:</b> Observed the location of backup tapes to determine that backup tapes were stored in a secure location and rotated offsite.	No Relevant Exception Noted
	<b>3b. Inspection:</b> Inspected offsite tape pickup logs to determine that data backup tapes were rotated offsite.	No Relevant Exceptions Noted
4. Access to data stored at the backup storage facility (Iron Mountain) is restricted to appropriate personnel.	<b>4a. Inquiry:</b> Inquired of the VP of Operations to determine appropriate personnel that should have access to recall IT related Media.	No Relevant Exception Noted
	<b>4b. Inspection:</b> Inspect authorization list to determine that only authorized personnel can recall files from the offsite backup database.	No Relevant Exceptions Noted

**Conclusion: Observed the application or existence of specific controls as represented.**

**Control Objective No. 5**

**Control activities provide reasonable assurance that systems are maintained in a manner that helps ensure system availability.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. System problems are tracked and monitored utilizing an online utility.	<b>1a. Inquiry:</b> Inquired of the IT Supervisor to determine the existence of a problem tracking system.	No Relevant Exception Noted
	<b>1b. Observation:</b> Observed the online system to determine that problems are logged.	No Relevant Exception Noted
2. Antivirus software is installed on all servers, personal computers, email servers and gateways.	<b>2a. Inspection:</b> Inspected system configurations to determine if antivirus software is installed on servers and workstations.	No Relevant Exception Noted
	<b>2b. Inspection:</b> Inspected system configurations to determine if antivirus software is installed on email servers and gateways.	No Relevant Exception Noted
3. A central server monitors for updates to antivirus definitions on an hourly basis. Updates are pushed to other servers and personal computers in the network.	<b>3a. Inspection:</b> Inspected antivirus configurations to determine if antivirus definitions are updated on an hourly basis.	No Relevant Exception Noted
	<b>3b. Inspection:</b> Inspected a judgmental sample of personal computers to determine that virus updates were current.	No Relevant Exception Noted
4. Service Pack/Patch Maintenance procedures exist to ensure updates are applied.	<b>4. Inspection:</b> Inspected Service Pack/Patch maintenance procedures to determine if procedures are formally documented.	No Relevant Exception Noted
5. IT personnel utilize automated utilities to identify vendor updates.	<b>5a. Inspection:</b> Inspected automated update utility configurations to determine that updates are pushed to corporate workstations.	No Relevant Exception Noted
	<b>5b. Inspection:</b> Inspected a judgmental sample of servers to determine if recent updates were applied.	No Relevant Exception Noted
<b>Conclusion: Observed the application or existence of specific controls as represented.</b>		

**Control Objective No. 6**

**Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. Corporate level information security policies and procedures are documented.	<b>1. Inspection:</b> Inspected the corporate level information security policies and procedures to verify existence.	No Relevant Exception Noted
2. An ID and password is required to access the DCL's backend databases.	<b>2a. Inquiry:</b> Inquired of the IT Supervisor to determine that an ID and password was required to access the database instances.	No Relevant Exception Noted
	<b>2b. Observation:</b> Observed an ID and password was required to access the database.	No Relevant Exception Noted
3. Direct access to the database instances are restricted and are limited based on job responsibility.	<b>3. Inspection:</b> Inspected database user access lists to determine that direct access to the database instances were restricted based on job responsibility.	No Relevant Exception Noted
4. An ID and password is required to access DCL's network operating systems.	<b>4a. Inquiry:</b> Inquired of the IT Supervisor to determine that an ID and password was required to access the DCL's network operating systems.	No Relevant Exception Noted
	<b>4b. Observation:</b> Observed an ID and password was required to access the network operating systems.	No Relevant Exception Noted
5. Number of Administrators is restricted to few authorized personnel.	<b>5. Inspection:</b> Inspected administrative access privileges to determine that access is limited to system administrators.	No Relevant Exception Noted
6. DCL's personnel are required to authenticate to the corporate network before accessing the DCL's application.	<b>6. Inspection:</b> Inspected network authentication configurations to determine that DCL's users were required to authenticate to the corporate network.	No Relevant Exception Noted
7. Network accounts are temporarily locked following a pre-defined number of failed login attempts.	<b>7. Inspection:</b> Inspected network authentication configurations to determine that network accounts were temporarily locked following a pre-defined number of failed login attempts.	No Relevant Exception Noted
8. DCL's personnel are not allowed to reuse a pre-defined number of previously used passwords.	<b>8. Inspection:</b> Inspected network authentication configurations to determine that DCL's personnel were not allowed to reuse a pre-defined number of previously used passwords.	No Relevant Exception Noted

9. Network account passwords expire at defined intervals.	<b>9. Inspection:</b> Inspected network authentication configurations to determine that network account passwords expired at defined intervals.	No Relevant Exception Noted
10. Network account passwords are required to adhere to a minimum length password.	<b>10. Inspection:</b> Inspected network authentication configurations to determine that network account passwords were required to adhere to minimum length passwords.	No Relevant Exception Noted
11. Network account passwords are required to meet certain complexity requirements.	<b>11. Inspection:</b> Inspected network authentication configurations to determine that network account passwords were required to meet certain complexity requirements.	No Relevant Exception Noted
<b>Conclusion: Observed the application or existence of specific controls as represented.</b>		

**Control Objective No. 7**

**Control activities provide reasonable assurance that changes to DCL's ERP On Demand application and supporting systems are properly authorized, tested, approved, implemented and documented.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Comments</b>
1. Application change management policies are formally documented.	<b>1. Inspection:</b> Inspected the DCL Policies and Procedures Manual version 3.1 January 1, 2006 to determine if existing application change management policies have been formally documented.	No Relevant Exception Noted
2. A process is in place to ensure that all changes are reviewed and approved by appropriate personnel.	<b>2a. Inspection:</b> Inspected the DCL Policies and Procedures Manual version 3.1 January 1, 2006 to determine if existing application change approval process is in place.	No Relevant Exception Noted
	<b>2b Inspection:</b> Inspected a judgmental sample of the Production Application Request form to determine proper approval and to determine if the change is entered into DCL Portal for monitoring.	No Relevant Exception Noted
3. Change requests undergo a priority assignment process.	<b>3. Observation:</b> Observed the DCL Portal system and noted if the priority assignment process is being followed.	No Relevant Exception Noted
4. There is a tracking process in place to ensure that changes to the production environment are documented and tracked.	<b>4. Observation:</b> Observed the DCL Portal system and noted if approved application change requests are assigned a reference tracking number to determine which application is being changed.	No Relevant Exception Noted
5. All changes are tested before being implemented in the production environment.	<b>5. Inspection:</b> Inspected a judgmental sample of the Status Updates and Testing Sub-page of change requests and noted if testing and user acceptance are logged	No Relevant Exception Noted
6. Developers are not given direct access to production environments.	<b>6. Inspection:</b> Obtained a list from IT Systems Supervisor the list of personnel who have access to production environment and ascertained that developers are not included in the list.	No Relevant Exception Noted
7. Policies and procedures related to emergency change requests are documented and in place.	<b>7. Inquiry:</b> Inquired of President and VP-IT/E-Commerce to determine if emergency application change requests policies and procedures are in place. Emergency change requests are managed via the same process as standard requests.	No Relevant Exception Noted

<p>8. All emergency change requests must receive approval from management prior to implementation.</p>	<p><b>8. Inquiry:</b> Inquired of President and VP-IT/E-Commerce to determine if emergency change requests are properly approved. Emergency change requests are managed via the same process as standard requests.</p>	<p>No Relevant Exception Noted</p>
<p><b>Conclusion: Observed the application or existence of specific controls as represented.</b></p>		

**Control Objective No. 8**

**Control activities provide reasonable assurance that the security infrastructure limits unauthorized access to internal networks and threats from connections to external networks are appropriately limited.**

Specified Controls	Test Performed by Service Auditor	Test Comments
1. Firewalls are placed to segment the network and protect its perimeter.	<b>1. Inspection:</b> Inspected the network diagram and physical hardware configuration to determine that firewalls are placed at the network perimeter and between sensitive zones.	No Relevant Exception Noted
2. Only authorized employees utilizing unique user ID's and passwords have the ability to change firewall rule sets.	<b>2a. Inquiry:</b> Inquired of the VP of Operations to determine that only authorized employees utilizing unique user ID's and passwords have the ability to change firewall rule sets.	No Relevant Exception Noted
	<b>2b. Inspection:</b> Inspected the group/user profiles to determine that only authorized personnel utilizing unique IDs and passwords have the ability to make changes.	No Relevant Exception Noted
3. A firewall log is in place to detect key intrusion notifications and is reviewed on a periodic basis by management.	<b>3a. Inquiry:</b> Inquired of the VP of Operations on the policy for review of the firewall log.	No Relevant Exception Noted
	<b>3b. Inspection:</b> Inspected the firewall log to determine that key intrusions were noted and reviewed on a periodic basis.	No Relevant Exception Noted

**Conclusion: Observed the application or existence of specific controls as represented.**

**Control Objective No. 9**

**Controls activities provide reasonable assurance that the Customer Inventory transactions are recorded by DCL in the Customer’s system in the appropriate period.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Results</b>
1. Inventory Control transacts Customer raw materials or RMAs as received based on receipt date indicated in the bill of lading or packing slip.	<b>1. Inspection:</b> Inspected a judgmental sample of raw materials or RMAs received in Customer’s system and traced the items to bill of lading or packing slip. Verified that the items are recorded when received.	No Relevant Exception Noted
2. Inventory Control transacts completed work orders as Customer’s finished goods based on Quality Assurance Group (QAG) approved work orders.	<b>2. Inspection:</b> Inspected a judgmental sample of completed work orders and verified that work orders are approved by QAG.	No Relevant Exception Noted
3. Shipping system automatically marks the goods to be shipped as complete upon being scanned by the RF gun.	<b>3. Observation:</b> Observed that the Shipping system automatically marks the goods to be shipped as complete after being scanned by the RF gun.	No Relevant Exception Noted
4. Shipping system detects if the picklist does not match the shipping box.	<b>4. Reperformance:</b> Reperformed scanning an erroneous shipping box and verified that the system would not allow the transaction to proceed.	No Relevant Exception Noted
5. Scanned shipments are shipped immediately. Unshipped goods are logged and reported to Customers in accordance with the established business rules.	<b>5. Inspection:</b> Inspected the “Left on Dock” log and verified its existence. Determined that items logged are immediately shipped and/or reported to the customer in accordance with the agreed-upon business rules.	No Relevant Exception Noted
<b>Conclusion: Observed the application or existence of specific controls as represented.</b>		

**Control Objective No. 10**

**Controls activities provide reasonable assurance that software keys are properly managed.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Results</b>
1. The printed software keys are stored in a locked cabinet that can only be accessed by few authorized personnel.	<b>1a. Observation:</b> Observed that the software keys are appropriately stored in a locked cabinet.	No Relevant Exception Noted
	<b>1b. Inquiry:</b> Performed corroborative inquiries to determine that keys to the cabinet are maintained only by few authorized employees.	No Relevant Exception Noted
2. The room containing the locked cabinet is monitored by surveillance cameras.	<b>2a. Observation:</b> Observed that surveillance monitoring is recorded.	No Relevant Exception Noted
	<b>2b. Inquiry and Inspection:</b> Performed collaborative inquiries to determine that the surveillance tapes are being reviewed. Inspected surveillance logs to determine that the cameras are timely reviewed.	No Relevant Exception Noted
3. Biometric devices control access to the room containing the software master keys.	<b>3a. Reperformance:</b> Attempted to access the room. Ascertained that access is appropriately restricted.	No Relevant Exception Noted
	<b>3b. Inspection:</b> Inspected access control list of the biometric device and ascertained that users who have access to the room have a valid business reason.	No Relevant Exception Noted
	<b>3c. Observation:</b> Observed that biometric device is used to control the access.	No Relevant Exception Noted
4. Access to downloading and printing of software keys are appropriately controlled and restricted. A second person verifies that only a specified number of keys are downloaded.	<b>4a. Inspection:</b> Inspected file verification log that documents the number of files downloaded and this is verified by a second person.	No Relevant Exception Noted
	<b>4b. Inspection:</b> Inspected access control list and ascertained that users who have access to print software keys are restricted.	No Relevant Exception Noted

**Conclusion: Observed the application or existence of specific controls as represented.**

**Control Objective No. 11**

**Controls activities provide reasonable assurance that Inventories are stored in a safe and secure location.**

<b>Specified Controls</b>	<b>Test Performed by Service Auditor</b>	<b>Test Results</b>
1. Cycle counts are performed for all customer inventories based on count frequencies communicated by the customer. For customers that have not communicated the count frequency, DCL performs the count at least once a month.	<b>1. Inspected:</b> Inspected judgmental sample of documentation that cycle counts are performed in accordance with the count frequencies communicated by the client; or evidence that the counts are performed at least once a month. For count discrepancies, determine that the discrepancies are appropriately resolved.	No Relevant Exception Noted
2. Customer inventories are properly labeled and properly segregated.	<b>2. Observation:</b> Observed segregation of inventories in the storage locations. Observed that inventories are properly labeled.	No Relevant Exception Noted
3. Environmental protection is adequately installed in the warehouse locations.	<b>3. Observation:</b> Observed that fire extinguishers, sprinklers, flow alarm, and temperature controls are strategically located within the warehouse facility.	No Relevant Exception Noted
4. Surveillance cameras are strategically located within the warehouse facility to monitor employee activity.	<b>4a Observation:</b> Observed that surveillance monitoring is recorded.	No Relevant Exception Noted
	<b>4b Inquiry:</b> Performed collaborative inquiries to determine that the surveillance tapes are being reviewed.	No Relevant Exception Noted
<b>Conclusion: Observed the application or existence of specific controls as represented.</b>		