



Independent Service Auditors' Report

DriveSavers Data Recovery, Inc.

Independent Service Auditors' Report on DriveSavers Data Recovery, Inc. Description of Its Data Recovery System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security Trust Services Criteria

For the Period May 1, 2020 to April 30, 2021



CliftonLarsonAllen LLP
Phoenix, Arizona



WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

CLAconnect.com

DRIVESAVERS DATA RECOVERY, INC.
TABLE OF CONTENTS

I. Independent Service Auditors' Report	1
II. Assertion of DriveSavers Data Recovery, Inc. Management	6
III. DriveSavers Data Recovery, Inc.'s Description of Its Data Recovery System.....	8
IV. Trust Services Category, Criteria, Related Controls, and Tests of Controls Relevant to Security	19
V. Other Information Provided by DriveSavers Data Recovery, Inc. That Is Not Covered by the Service Auditors' Report.....	54



CliftonLarsonAllen LLP
20 East Thomas Road, Suite 2300
Phoenix, Arizona 85012

phone 602-266-2248 fax 602-266-2907
CLAcconnect.com

I. Independent Service Auditors' Report

Executive Committee
DriveSavers Data Recovery, Inc.
Novato, California

Scope

We have examined DriveSavers Data Recovery, Inc.'s accompanying description of its Data Recovery system titled "DriveSavers Data Recovery, Inc.'s Description of Its Data Recovery System" throughout the period May 1, 2020 to April 30, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2020 to April 30, 2021, to provide reasonable assurance that DriveSavers Data Recovery, Inc. service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

DriveSavers Data Recovery, Inc. uses a subservice organization to provide IT managed services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DriveSavers Data Recovery, Inc., to achieve DriveSavers Data Recovery, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents DriveSavers Data Recovery, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at DriveSavers Data Recovery, Inc., to achieve DriveSavers Data Recovery, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents DriveSavers Data Recovery, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.



CLA is an independent member of Nexia International, a leading, global network of independent accounting and consulting firms. See [nexia.com/member-firm-disclaimer](https://www.nexia.com/member-firm-disclaimer) for details.

Service Organization's Responsibilities

DriveSavers Data Recovery, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that DriveSavers Data Recovery, Inc.'s service commitments and system requirements were achieved. DriveSavers Data Recovery, Inc. has provided the accompanying assertion titled "Assertion of DriveSavers Data Recovery, Inc. Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. DriveSavers Data Recovery, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

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

- Obtaining an understanding of the system and the services organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also includes performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in section IV.

Basis for Qualified Opinion

DriveSavers Data Recovery, Inc. states in the description of its system that new hires and current employees acknowledge upon hire and re-affirm policies and procedures annually, including the Acceptable Use Policy and Code of Conduct. Additionally, a tracking tool is used to monitor compliance with said acknowledgements. However, as noted on page 20 of the description of tests of controls and the results thereof, controls related to the new hire and current employee acknowledgements and compliance tracking were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-1.1, The entity demonstrates a commitment to integrity and ethical values.

DriveSavers Data Recovery, Inc. states in the description of its system that employee training and policy compliance is tracked. However, as noted on page 24 of the description of tests of controls and the results thereof, controls related to training and policy compliance tracking were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-1.4, The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

DriveSavers Data Recovery, Inc. states in the description of its system that new hires and current employees acknowledge upon hire and re-affirm policies and procedures annually, including the nondisclosure of information agreement. However, as noted on page 26 of the description of tests of controls and the results thereof, controls related to the new hire and current employee acknowledgements were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-2.2, The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

DriveSavers Data Recovery, Inc. states in the description of its system that all security policies and procedures are reviewed annually, and the code of conduct is signed by new hires and current employees. However, as noted on page 35 of the description of tests of controls and the results thereof, controls related to the annual review of security policies and procedures and code of conduct acknowledgements were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-5.3, The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Opinion

In our opinion, except for the possible effects of the matters giving rise to the modification described in the preceding paragraphs, in all material respects —

- a. the description presents DriveSavers Data Recovery, Inc.'s Data Recovery system that was designed and implemented throughout the period May 1, 2020 to April 30, 2021, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period May 1, 2020 to April 30, 2021, to provide reasonable assurance that DriveSavers Data Recovery, Inc. service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period May 1, 2020 to April 30, 2021, to provide reasonable assurance that DriveSavers Data Recovery, Inc. service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls operated effectively throughout that period.

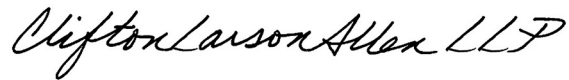
Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of DriveSavers Data Recovery, Inc., user entities of DriveSavers Data Recovery, Inc. Data Recovery system during some or all of the period May 1, 2020 to April 30, 2021, business partners of DriveSavers Data Recovery, Inc. subject to risks arising from interactions with the Data Recovery system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations

- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



CliftonLarsonAllen LLP

Phoenix, Arizona

August 10, 2021



II. Assertion of DriveSavers Data Recovery, Inc. Management

Management of DriveSavers Data Recovery, Inc. Assertion Regarding Its Data Recovery System for the Period May 1, 2020 to April 30, 2021

Assertion of the Management of DriveSavers Data Recovery, Inc.

We have prepared the accompanying description of DriveSavers Data Recovery, Inc.'s Data Recovery system titled "DriveSavers Data Recovery, Inc.'s Description of its Data Recovery System" throughout the period May 1, 2020 to April 30, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Data Recovery system that may be useful when assessing the risks arising from interactions with DriveSavers Data Recovery, Inc.'s system, particularly information about system controls that DriveSavers Data Recovery, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, *Trust Services Criteria*).

DriveSavers Data Recovery, Inc. uses a subservice organization to provide managed IT services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DriveSavers Data Recovery, Inc., to achieve DriveSavers Data Recovery, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents DriveSavers Data Recovery, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at DriveSavers Data Recovery, Inc., to achieve DriveSavers Data Recovery, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents DriveSavers Data Recovery, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls.

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

- a. the description presents DriveSavers Data Recovery, Inc.'s Data Recovery system that was designed and implemented throughout the period May 1, 2020, to April 30, 2021, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that XYZ's service commitments and system



requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls throughout that period.

- c. Except for the matter described in the following paragraphs, the controls stated in the description operated effectively throughout the period May 1, 2020, to April 30, 2021, to provide reasonable assurance that DriveSavers Data Recovery, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of DriveSavers Data Recovery, Inc.'s controls operated effectively throughout that period except as noted below.
- d. As noted on page 22 of the description of tests of controls and the results thereof, controls related to the new hire and current employee acknowledgements and compliance tracking were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-1.1, The entity demonstrates a commitment to integrity and ethical values.

As noted on page 26 of the description of tests of controls and the results thereof, controls related to training and policy compliance tracking were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-1.4, The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

As noted on page 28 of the description of tests of controls and the results thereof, controls related to the new hire and current employee acknowledgements were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-2.2, The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

As noted on page 37 of the description of tests of controls and the results thereof, controls related to the annual review of security policies and procedures and code of conduct acknowledgements were not consistently performed and, therefore, were not operating effectively throughout the period May 1, 2020 to April 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC-5.3, The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

III. DriveSavers Data Recovery, Inc.’s Description of Its Data Recovery System

Organization Background

Company Profile

Founded in 1985, DriveSavers Data Recovery Inc. (DriveSavers) is a data recovery firm serving all forms of businesses that require data recovery. DriveSavers provides trusted and proven data recovery technology solutions including recovery of RAID, NAS, SAN, tape and multi-disk systems.

Business Services

DriveSavers provides data recovery firm serving all forms of businesses that require data recovery. Their dedicated team of experienced enterprise engineers combines proprietary software and hardware tools with multi-terabyte systems to achieve amazing results, even from storage devices with mechanical failure or physical damage. The following manufacturers prefer DriveSavers for the recovery of their servers and storage devices: Dell, HP/Compaq, and Apple. Leading manufacturers authorize DriveSavers to open sealed drive mechanisms without voiding the original warranty.

Specific service offerings include:

Service Offering(s)	Service Description
Data recovery of	<ul style="list-style-type: none"> • RAID • NAS • SAN • TAPE • MULTI-DISK • CD • DVD • REMOVABLE MEDIA - THUMB DRIVES • HANDHELD (PDA’s / IPODS / CELL PHONES / TABLETS) • DESKTOPS • LAPTOPS • DIGITAL CAMERAS • DIGITAL ARTS RECOVERY • FILE LEVEL AND DISK LEVEL ENCRYPTED DATA

DriveSavers has established a relationship with the following business partners for delivery of services:

Vendor Name	Service(s) Provided
Computer Services, Inc. (CSI)	Managed IT Services Provider

Products/services obtained from third-party business partners related to delivery of DriveSavers products/services to clients are supported by documentation outlining services provided by third party.

Data Type(s)

Electronic data involved with the delivery of DriveSavers Data Recovery Inc.' products/services is primarily public information. The exception to this statement is income information that is provided on the form 4506-T and social security verifications form both of which are completed by the consumer.

System Description

The definition of "system" specific to this engagement consists of five key components and is described as follows:

- **Infrastructure** The physical and hardware components of a system (facilities, equipment, and networks)
- **Software** The programs and operating software of a system (systems, applications, and utilities)
- **Data** The information used *and supported* by a system (transaction streams, files, databases, and tables)
- **People** The personnel involved in the operation and use of a system (developers, operators, users, and managers)
- **Procedures** The automated and manual procedures involved in the operation of a system

On the following pages, DriveSavers has provided a description of each system component. In addition, the procedures described by DriveSavers cross reference the relevant criteria specific to the selected Trust Principle(s).

Infrastructure

The physical and hardware components of a system (facilities, equipment, and networks)

Facility

DriveSavers, Inc. maintains a secured headquarters in Novato, California. The facility is physically secured and environmentally controlled with card access badges, closed circuit television cameras, temperature and humidity controls, fire prevention and suppressions systems, intruder alarms and backup electrical power. DriveSavers is Department of Defense (DOD) Certified.

Building Security

All exterior doors remain locked at all times. DriveSavers employees are issued access control cards or FOBs to enter the building. Access to internal areas is granted on an as needed basis based upon employee's job function.

Visitors

All external entrances are locked, requiring visitors to DriveSavers Data Recovery Inc. to utilize a camera-controlled Intercom system to request access to the facility. All visitors must sign in at the reception desk and be issued a visitor's badge. Visitors are escorted by DriveSavers Data Recovery Inc. Services staff while onsite. Visitors are required to sign out when leaving the facility.

Restricted Areas

Within the building, the lab areas and IT network computer room have been designated as "Restricted" and require an additional level of security to access the area. All access points to Restricted Areas requiring proximity card access are logged.

Equipment

All equipment used in support of production operations is located within DriveSavers Data Recovery Inc. Services and managed by internal personnel resources. On an as-needed basis, hardware vendors will provide on-site and/or remote support and assistance for troubleshooting and ongoing maintenance activities. Categories of equipment include the following:

Communications Equipment

Routers, switches and other communication devices are installed within DriveSavers Data Recovery Inc. Services to manage data traffic internally within the facility and incoming/outgoing data transmissions.

Server(s)

Servers utilized by DriveSavers Data Recovery Inc. for production processing are a combination of physical servers and virtual servers utilizing VMWare / HyperV. Additional and replacement servers are purchased by DriveSavers Data Recovery Inc. from Fortune500 manufacturers.

User Computing Device(s)

Desktop and laptop workstations owned by DriveSavers Data Recovery Inc. Services are used for production processing purposes.

Network

Connectivity

Circuits

Connection to the Internet is dependent on following methods:

- T-1
- Cable

DriveSavers Data Recovery Inc. maintains redundant communications to the Internet for failover purposes. This redundant connection enters the server room through diverse communication channels.

Internal (Production) Network

Access to the internal network occurs via a wired connection based on TCP/IP protocol. DriveSavers Data Recovery Inc. Services maintains a network of wired routers, firewalls, switches, load balancers and VPN appliances providing network connectivity to five separate networks. DriveSavers Data Recovery Inc. has not implemented a wireless network for production or guest services.

Security Devices

Firewall

Connections to and from DriveSavers Data Recovery Inc. Services' networks are protected by firewalls that are hosted and managed internally.

DMZ

A demilitarized zone (DMZ) is used to separate publicly accessible servers from the trusted network. These DMZs only allow authorized traffic to pass in and out of the DMZ.

Remote Access

Capability to connect to the DriveSavers Data Recovery Inc. network remotely is accomplished via third-party software that creates a secure VPN tunnel.

Employees

DriveSavers Data Recovery Inc. employees that have a business need to connect remotely are required to establish the connection via a VPN session. Employees must obtain approval from the business unit manager of DriveSavers Data Recovery Inc. prior to being authorized to access the network remotely. Access is controlled by a security group in Active Directory. Employees are required to enter their username and password when initiating the VPN and provide an MFA authentication code.

Vendors

Remote access to the DriveSavers Data Recovery Inc. network is limited to the specific named vendor users. Access is controlled by DriveSavers Data Recovery Inc. and is only given when needed. Once the security system vendor is finished access is removed again.

Software

The programs and operating software of a system (systems, applications, and utilities)

Software Administration

Software Inventory

DriveSavers Data Recovery Inc. has identified all business-critical applications including product name, developer, license number and related terms and maintains this information in a central repository.

License Administration

A copy of the executed license agreement is maintained by the IT Manager who is also responsible for ensuring compliance with license terms and use rights.

Maintenance / Support

Maintenance of Microsoft applications is included as part of the software licensing agreement.

Operating System(s) Software

Overview

Similar to equipment, operating system software that has been installed on production servers is administered by internal personnel resources. On an as-needed basis, software vendors will provide remote support and assistance for troubleshooting and software updates/patches.

Servers

DriveSavers Data Recovery Inc. Services has implemented and maintains current vendor supported operating system for Microsoft Windows server to support production and nonproduction operations.

User Computing Device(s)

Microsoft Windows operating system software has been installed on desktop and laptop workstations in support of production and nonproduction operations.

Security Software

Security software has been installed on servers and workstations to protect data and the underlying infrastructure from unauthorized access and activity within production and nonproduction systems and includes but is not limited to the following:

- Anti-Virus/Malware

- Intrusion Detection / Intrusion Prevention
- Event Monitoring
- Event Alerting
- Centralized Logging
- Web Filtering

System Utilities

Utilities to support production systems include but are not limited to the following:

- System Performance and Availability Monitoring Software
- Backup Software
- User Authentication & Identification (Physical & Logical)

Data

The information used and supported by a system (transaction streams, files, databases, and tables)

Client Data Administration

Data Classification

Data follows a classification schema that describes the security and handling of data. Classifications include:

Classification	Description
Confidential	All customers' data is treated as confidential.

Overview

The company transmits and receives all client data externally via courier services for receiving and sending data using encryption technology whenever possible.

People

The personnel involved in the operation and use of a system (developers, operators, users, and managers)

DriveSavers Data Recovery Inc. Services Employees

DriveSavers Data Recovery Inc. has a staff of 85 full- and part-time employees that are assigned to various roles within the organization. Overall, the President is responsible for administration of DriveSavers Data Recovery Inc.

DriveSavers Data Recovery Inc. personnel resources that are assigned to one of the following functional business areas:

Business Function(s)	Responsibility
Shipping	Arranges the collection and shipping of storage media from various courier services

Business Function(s)	Responsibility
Information Technology	Oversees the installation and maintenance of the computer network and infrastructure
Data Recovery	Performs the data recovery of client’s information
Security Compliance	Makes sure business is conducted in full compliance with all laws and regulations and maintains a safe and secure environment

IT Support Service

IT Support staff is responsible for troubleshooting issues reported by internal users, business partners and clients. The DriveSavers Data Recovery Inc. Help Desk is staffed from 6:00 AM through 5:00 PM Pacific Time, Monday through Friday, and no weekend staffing. Issues that are reported outside of this schedule are reviewed by IT personnel and prioritized and reacted to base on severity and the DriveSavers Data Recovery Inc. to the business.

Contracted Personnel

DriveSavers Data Recovery Inc. Services supplements current staff with contracted personnel resources when: 1) unique skills are not resident within DriveSavers Data Recovery Inc. Services or 2) deadlines cannot be met with existing employees.

Procedures

The automated and manual procedures involved in the operation of a system

Procedures related to Order Fulfillment Services are described in a sequence relevant to the Trust Principles and Criteria in scope of this engagement including:

Systems Security

Management has developed and communicated procedures relevant to systems security to employees, clients and external business partners to restrict logical access to the DriveSavers Data Recovery Inc. Services system. Procedures are reviewed annually by functional business area leads with changes approved by management. These procedures cover the following key elements of systems security:

- Selection, documentation, and implementation of security controls related to:
 - Network(s) / Security Device(s) / Server(s) / Workstation(s)
 - Database(s) / Application System(s)
 - Facilities
- Systems Security Configuration / Patching
- Managing Systems User Account Access
- Monitoring Systems Security-related Activity

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls

Control Environment

Organization Structure

The organization structure of DriveSavers provides the overall framework for establishing, directing, and monitoring strategic objectives. The overall hierarchy and individual reporting relationships have been established to support and promote operational independence between functions areas of the organization and underlying roles and responsibilities.

Management Philosophy

DriveSavers operates in an industry where risk management, control, and reputation are critical. The company has instituted policies and programs to promote an appropriate control environment in support of customer needs. The primary elements of DriveSavers control environment are demonstrated by management's philosophy and operating style; management's integrity and ethical values; the method of assignment of authority, responsibility and close supervision; human resources, skills and commitments to competence; information risk management; and the company's organizational structure, reporting mechanisms and segregation of duties; management's controls for monitoring and following up on performance, including the results of internal controls procedures; and management's response to various external influences that affect the company's operations such as examinations by independent third parties.

Strategic Planning

The control environment sets the tone of the organization, influencing the control consciousness of all personnel. It is the foundation for all other components of internal control, providing discipline and structure. Through the control environment, management influences the way business activities are structured, objectives are established, and risks are assessed. It influences control activities, information and communication systems, and monitoring procedures. DriveSavers managerial culture instills a companywide attitude of integrity, security, and control consciousness, and sets a positive "tone at the top". Management has established methods that foster shared values and teamwork in pursuit of these objectives.

Integrity and Ethical Values

Specific control activities that DriveSavers implemented in this area are described below.

- Code of conduct and behavioral standards are documented and communicated to personnel.
- The employee policy and procedures contain organizational policy statements and codes of conduct to which all employees and contractors are required to adhere.
- Personnel acknowledge relevant policies and procedures, confirming they have been given access and understand their responsibility for adhering to requirements within.
- All personnel must sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Since November 2007, background checks are performed for all employees and contractors as a component of the hiring process and are also conducted annually for all employees.

Risk Assessment Process

DriveSavers has placed into operation an annual risk assessment program to identify and manage risks that could affect DriveSavers ability to properly control its assets and to serve its customers. This program requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address and mitigate those risks. Company meetings include a discussion of these matters. DriveSavers has identified various internal and external risk factors. DriveSavers has assessed the

probable impact of the events in their probability of occurrence and has implemented various measures designed to manage those risks. Risks that are considered during management's formal and informal risk assessment activities may include consideration of the following events:

- Changes in operating environment
- New personnel
- New or changed information systems
- Rapid growth/decline
- New business models, products, or activities
- Corporate restructurings
- Expanded operations

Information and Communication

DriveSavers has implemented various methods of communication to help ensure employees understand their individual roles and internal controls, and to facilitate the timely dissemination of significant events. Time sensitive information is communicated directly to employees and via e-mail. Employees are required to adhere to DriveSavers policies and procedures to ensure that records and other documents are maintained accurately, securely and completely. DriveSavers facilitates the effective flow of information through key business performance metrics and system related metrics. There is also an "open door" policy that allows employees direct access to the management team.

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within the company. DriveSavers management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organization charts and acceptable use policies are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

Monitoring of Controls

Monitoring requires a clear understanding of processes and their relationships to key risks, progress towards addressing the highest rated risks, and ongoing risk assessment and effectiveness of managing risk. DriveSavers management performs monitoring activities in order to continuously assess the quality of internal controls over time. Monitoring activities are used to initiate corrective actions through department meetings, client conference calls, and informal notifications. Monitoring activities are conducted on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any control weaknesses is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Additionally, DriveSavers personnel monitor the quality of internal control and operating performance as a normal part of their business activities. Key business metrics and IT metrics are maintained to facilitate this monitoring process. Exceptions and deviations to normal business activity are reviewed by management and sufficiently resolved. Management strives to provide accurate information and tools to employees to facilitate compliance with policies and procedures that help manage risk.

Control Activities

Policy Statements, Standards & Procedures

DriveSavers has established operating policies and procedures for use by employees. The management committee maintains policies and procedures related to system administration, use, controls and operating procedures. Policies and procedures are updated as warranted and appropriate personnel are notified when policy or procedure has changed.

Personnel Administration

Management of DriveSavers Data Recovery Inc. has a strong commitment to recruit, develop, and retain competent personnel to execute the business plan to achieve business and control objectives. Most staff positions are filled through general solicitation or employee referrals. Management positions are commonly filled through employee performance growth and referrals. Employment with DriveSavers Data Recovery Inc. is "at will" and is stated in the employment application.

Candidates for open positions are interviewed and hired based on their qualifications to satisfy the requirements of the position as outlined in the job description. DriveSavers Data Recovery Inc. maintains documentation for each employee in a personnel file including:

- Identification of Department
- Employment Application
- Background Check Consent Form / Results
- Acknowledgment of receipt of the Employee Handbook including Workplace Rules

Employee Separation

DriveSavers Data Recovery Inc. has established a checklist that identifies steps associated with the employee termination process. The checklist addresses both voluntary resignations and involuntary terminations. Completion of the checklist and all separation related activities is the responsibility of the business unit manager including notifying IT to disable/remove user accounts, retrieving physical security access devices and DriveSavers Data Recovery Inc.-owned technology assets.

Contracted / Temporary Personnel

Contracted and temporary personnel resources used to satisfy short-term staffing needs and specific project requirements must be approved by the project manager and HR department.

System(s) Development & Change Management

DriveSavers requires that internal changes to its systems be documented and approved by management. Changes are scheduled to reduce disruptions. The individual migrating the change into production is approved by management. Documentation of changes and associated authorizations are retained in a centralized location for ease of administration. Internal changes are moved to production by authorized personnel. Management reviews the access to production systems for appropriateness of personnel.

System(s) Account Management

DriveSavers maintains corporate policies, procedures, and controls to facilitate logical security. The company performs a risk assessment to identify potential business and security risks and implements measures to reduce the risks. There is a Corporate Code of Conduct that each employee signs, along with policies for security, confidentiality, nondisclosure, and acceptable use of systems. There are security administration procedures that require management's authorization for any add, change, and delete of user accounts. Segregation of IT duties is achieved by the ongoing review of employee access rights. DriveSavers employees are authorized by management to access information of their systems and their clients' systems based upon their job requirements. Best practices are employed by DriveSavers for password administration. Passwords

are confidential, not shared, are complex, and must be changed after a prescribed time period. Passwords are required to have a sufficient number of characters. Default passwords are changed. DriveSavers uses a virtual private network (VPN) and firewalls for secure access through the Internet. Remote users are authorized by management.

Data Backup and Recovery

DriveSavers uses automated systems for scheduling tasks such as backups. Backups are taken on a nightly basis, with the backup media stored in a secure off-site facility. Backup logs are monitored to ensure completeness of processing. The company periodically tests the backup media to facilitate its recoverability.

Physical Security and Environmental Controls

The facility is physically secured and environmentally controlled with card access badges, closed circuit television cameras, temperature and humidity controls, fire prevention and suppressions systems, intruder alarms and backup electrical power. DriveSavers is Department of Defense (DOD) Certified.

Security Monitoring & Response

Remote user access is logged and reviewed monthly. DriveSavers monitors their security stringently. Intrusion prevention and detection systems are installed and continuously monitored. Security alerts are identified, escalated, and communicated. Remedial action is taken if necessary. DriveSavers employs automated preventative controls to minimize disruptions from computer viruses and spyware. The network is periodically assessed by an independent third party for system configuration errors and vulnerabilities. Additionally, DriveSavers external audit team completes regular self-assessments of DriveSavers controls.

Problem Management / Notification

DriveSavers computers at the headquarters are processing their operations on a 24/7/365 basis. Processes are in place to minimize interruptions in service. A help desk is maintained via the MAC and PC engineering group, along with a system that tracks the status and resolution of calls to the help desk and reported problems.

Complementary Subservice Organization Controls

DriveSavers has relationships with the following subservice organization (vendor) for the delivery of services.

Criteria		Control(s) Responsibility
Computer Services, Inc. (CSI)		
CC-6.4	Physical Security	<ul style="list-style-type: none"> Physical Security of Data Centers
CC-4.1	Monitoring of Controls	<ul style="list-style-type: none"> 24/7 Network monitoring and alerting
CC-3.1 CC-3.2	Threat Analysis & Risk Mitigation Strategies	<ul style="list-style-type: none"> Conduct and perform IT Risk Assessment
CC-7.1	Vulnerabilities	<ul style="list-style-type: none"> Perform external and internal vulnerabilities scans

Complementary User Entity Controls

DriveSavers services are designed with the assumption that certain controls will be implemented by client organization. Companies will abide by all regulatory controls and follow industry best practices. Such controls are called complementary client organization controls. It is not feasible for all of the control objectives related to DriveSavers services to be solely met the applicable trust services criterion. Accordingly, client organizations, in conjunction with the services, should follow their own internal controls and procedures to complement those of DriveSavers.

The following complementary client organization controls should be implemented by client organizations to provide additional assurance that the trust services criterion described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the client organizations, client organizations’ auditors, compliance officers, and security officers should exercise judgment in selecting and reviewing these complementary client organization controls.

Criteria	Customer User Entity Control(s)
CC-2.3	<ul style="list-style-type: none"> Client organizations are responsible for understanding and complying with their contractual obligations to DriveSavers.
CC-6.1	<ul style="list-style-type: none"> Client organizations are responsible for ensuring the confidentiality of any user IDs and passwords given to DriveSavers.
CC-2.3	<ul style="list-style-type: none"> Client organizations are responsible for maintaining their own system(s) of record.
CC-3.1	<ul style="list-style-type: none"> Client organizations are responsible for determining whether DriveSavers security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.
CC-2.3	<ul style="list-style-type: none"> Client organizations are responsible for complying with DriveSavers Data Recovery Inc. process.
CC-7.2	<ul style="list-style-type: none"> Client organizations are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize DriveSavers services.
CC-7.2	<ul style="list-style-type: none"> Client organizations are responsible for defining backup schedules and backing up their data.
CC-6.1	<ul style="list-style-type: none"> Client organizations are responsible for providing redundant infrastructure as needed.
CC-5.2	<ul style="list-style-type: none"> Client organizations are responsible for defining and implementing operating system, application, and database controls.

IV. Trust Services Category, Criteria, Related Controls, and Tests of Controls Relevant to Security

<p>Common Criteria Common Criteria to Security Category of the Trust Services Criteria</p>

CC-1.0 CONTROL ENVIRONMENT– Common Criteria Related to Control Environment			
CC-1.1 The entity demonstrates a commitment to integrity and ethical values.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.1.1	Personnel are required to read and accept the approved policies and procedures upon their hire and to formally re-affirm them annually thereafter.	<p>Inquired of management determine that new hires did not read and accept the approved policies and procedures during the reporting period.</p> <p>Inquired of management to determine that existing employees did not read and accept the approved policies and procedures during the reporting period.</p>	<p>Exception Noted.</p> <p>Ten out of ten current employees that were selected for testing did not re-affirm the annual policies and procedures.</p> <p>Two out of two new hires that were selected for testing did not read and accept the approved policies and procedures upon their hire.</p>
CC-1.1.2	Personnel are required to read and accept the corporate Acceptable Use policy upon their hire and to formally re-affirm them annually thereafter.	<p>Inspected acknowledgement forms for a selection of new hires during the reporting period to determine that employees read and accepted the corporate Acceptable Use policy.</p> <p>Inspected annual acknowledgement forms for selection of existing employees to determine that employees read and accepted the corporate Acceptable Use policy.</p>	<p>Exception Noted.</p> <p>Six out of ten current employees that were selected for testing did not re-affirm the acceptable use policy during the audit period.</p> <p>One out of two new hires that were selected for testing did not sign the acceptable use policy upon their hire.</p>

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.1.3	Personnel are required to read and accept the code of conduct upon their hire and to formally re-affirm them annually thereafter.	<p>Inspected acknowledgement forms for a selection of new hires during the reporting period to determine that employees read and accepted the code of conduct.</p> <p>Inspected annual acknowledgement forms for a selection of existing employees to determine that employees read and accepted the code of conduct.</p> <p>Inspected DriveSavers' Acceptable Use Policy to determine that Code of Conduct was included in the form.</p>	<p>Exception Noted.</p> <p>Six out of ten current employees did not re-affirm on code of conduct during the audit period.</p> <p>One out of two new hires that were selected for testing did not read and accept the code of conduct upon their hire.</p>
CC-1.1.4	A tracking tool is used to monitor compliance with new hire and annual acknowledgements.	Inquired of management to determine new hire and annual acknowledgements were not tracked during the period.	<p>Exception Noted.</p> <p>A tracking tool was not used to monitor compliance with acknowledgements during the reporting period.</p>
CC-1.1.5	All employees (full-time, part-time, and/or contractor) must pass an initial criminal background check before being employed. Thereafter, an annual background check will be conducted for all employees.	Inspected background checks from Human Resource files for a selection of new hires to determine initial criminal background checks were conducted.	No Exceptions Noted

CC-1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.2.1	Executive Committee oversees the strategic direction, plans, budgets, and the daily operations of the company.	Inspected security policies to determine that the strategic direction, plans, budgets, and daily operations were assigned to the Executive Committee.	No Exceptions Noted
CC-1.2.2	Roles and responsibilities of the board, management, users, vendors, and others, including but not limited to approval and responsibilities defined in the security policies.	Inspected security policies to determine that the board, management, users, vendors, and other roles and responsibilities were defined in the security policies.	No Exceptions Noted
CC-1.2.3	At the Monthly Manager Meetings, management evaluates the need for changes and re-alignment of the organization structure and reporting.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that needs for changes and re-alignment of the organization structure and reporting were discussed in the Monthly Manager Meetings.	No Exceptions Noted

CC-1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.3.1	DriveSavers has its organizational structure, reporting lines, authorities, and responsibilities defined in an organization chart.	Inspected the organization chart to determine that organizational structure, reporting lines, authorities, and responsibilities were defined.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.3.2	At the Monthly Manager Meetings, management evaluates the need for changes and re-alignment of the organization structure and reporting.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that needs for changes and re-alignment of the organization structure and reporting were discussed in the Monthly Manager Meetings.	No Exceptions Noted
CC-1.3.3	Roles and responsibilities of the board, management, users, vendors, and others, including but not limited to approval and responsibilities defined in the security policies.	Inspected security policies to determine that the board, management, users, vendors, and other roles and responsibilities were defined in the security policies.	No Exceptions Noted
CC-1.3.4	Executive Committee oversees the strategic direction, plans, budgets, and the daily operations of the company.	Inspected security policies to determine that the strategic direction, plans, budgets, and daily operations were assigned to the Executive Committee.	No Exceptions Noted

CC-1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.4.1	Job postings outline the minimum experience and training requirements for the posting.	Inspected job postings for all job positions to determine that minimum experience and training requirements were defined.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.4.2	DriveSavers employees attend annual security awareness training and policy compliance. Record of attendance is retained through a tracking tool.	Inspected the training agenda for annual training to determine it included security awareness topics. Inspected the training tracking document to determine that all DriveSavers employees attended annual security awareness training.	Exception Noted. All employees were required to undergo security awareness training; however, employee policy compliance was not tracked during the reporting period.
CC-1.4.3	A tracking tool is used to monitor compliance with annual training requirements.	Inquired of management to determine that compliance with annual training requirements were not monitored during the period.	Exception Noted. Employee training compliance was not tracked during the reporting period.
CC-1.4.4	At Monthly Manager Meetings, the need for additional resources and skills are discussed in order to achieve business objectives.	Inspected meeting minutes from Monthly Manager Meeting for a selection of months to determine that needs for additional resources and skills were discussed in the Monthly Manager Meetings.	No Exceptions Noted

CC-1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-1.5.1	Roles and responsibilities of the board, management, users, vendors, and others, including but not limited to approval and responsibilities defined in the security policies.	Inspected security policies to determine that the board, management, users, vendors, and other roles and responsibilities were defined in the security policies.	No Exceptions Noted
CC-1.5.2	DriveSavers conducts an annual review of all security policies and procedures.	Inspected information security policies to determine that an annual review was performed.	Exception Noted. There was no annual review of all security policies and procedures.

CC-2.0 Communication and Information			
CC-2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-2.1.1	At the Monthly Manager Meetings, management evaluates the detail graphs and spreadsheets about the business operations and performances.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that management evaluated the detail graphs and spreadsheets about the business operations in the Monthly Manager Meetings.	No Exceptions Noted
CC-2.1.2	At the Monthly Manager Meetings, management discuss the monthly statistics from the IT service provider.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that the monthly statistics from the IT service provider were discussed in the Monthly Manager Meetings.	No Exceptions Noted
CC-2.1.3	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted

CC-2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-2.2.1	Personnel are required to read and accept the approved policies and procedures upon their hire and to formally re-affirm them annually thereafter.	<p>Inquired of management determine that new hires did not read and accept the approved policies and procedures during the reporting period.</p> <p>Inquired of management to determine that existing employees did not read and accept the approved policies and procedures during the reporting period.</p>	<p>Exception Noted.</p> <p>Current employees did not re-affirm the annual policies and procedures.</p> <p>New Hires did not read and accept the approved policies and procedures upon their hire.</p>
CC-2.2.2	Personnel are required to read and sign nondisclosure of information agreement upon their hire and to formally re-affirm them annually thereafter.	<p>Inspected acknowledgement forms for a selection of new hires during the reporting period to determine that nondisclosure of information agreement was signed.</p> <p>Inspected acknowledgment forms for selection of current employees during the reporting period to determine that the nondisclosure of information agreement was signed.</p>	<p>Exception Noted.</p> <p>Eight out of ten existing employees did not re-affirm the nondisclosure of information agreement during the review period.</p>
CC-2.2.3	Communication of relevant company information to employees is via the CRM application and email communication as outlined in the security policies.	Inspected chief information security officer's inbox with a search of key words "policy, procedure and changes" to determine no changes occurred.	<p>No communication to employees regarding policies occurred during the reporting period.</p> <p>As a result, no testing of operating effectiveness was performed.</p>

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-2.2.4	A description of the system is posted on DriveSavers' CRM application and is available to DriveSavers' employees. All relevant procedures associated with the drive recovery services are located here.	Inspected Engineering WIKI to determine that a description of the system was posted and was available to DriveSavers' employees.	No Exceptions Noted
CC-2.2.5	Procedures documents for problem management processes, which include responsibility for reporting problems (and the process for doing so).	Inspected procedures to determine that procedures were documented for problem management and outlined the responsibility for reporting problems.	No Exceptions Noted

CC-2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-2.3.1	DriveSavers has provided descriptions of the drive recovery service(s) and plan(s) that DriveSavers offers on its external website.	Inspected the content of the external website to determine that description of the drive recovery service(s) and plan(s) were on the external website.	No Exceptions Noted
CC-2.3.2	DriveSavers security commitments regarding the service are included in the introductory message and statement of work.	Inspected the introductory email and statement of work to determine security commitments regarding services were included.	No Exceptions Noted
CC-2.3.3	Procedures documents for problem management processes, which include responsibility for reporting problems (and the process for doing so).	Inspected procedures to determine that procedures were documented for problem management and outlined the responsibility for reporting problems.	No Exceptions Noted

CC-3.0 Risk Assessment			
CC-3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.1.1	An assessment of DriveSavers' risks is performed on an annual basis, and documented procedures, processes and controls for reducing the identified risks.	<p>Inspected the annual risk assessment to determine that the assessment was performed on an annual basis.</p> <p>Inspected IS Policies to determine that procedures, processes and controls were documented for reducing the identified risks.</p>	No Exceptions Noted
CC-3.1.2	Identified risks are rated using a risk evaluation process and ratings are reviewed by management annually at the Monthly Management Meeting.	Inspected meeting minutes from the Manager Meetings to determine that risks were rated using a risk evaluation process and ratings and were reviewed by management annually.	No Exceptions Noted
CC-3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.2.1	An assessment of DriveSavers' risks is performed on an annual basis, and documented procedures, processes and controls for reducing the identified risks.	<p>Inspected the annual risk assessment to determine that the assessment was performed on an annual basis.</p> <p>Inspected IS Policies to determine that procedures, processes and controls were documented for reducing the identified risks.</p>	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.2.2	For items assessed, the risk assessment includes identification of business criticality; data sensitivity; relevant threats assessed; inherent and residual risk for each threat assessed; and identification of relevant business impact areas for each threat (financial, legal, compliance, reputation, and operations).	Inspected the annual risk assessment to determine that threats were assessed by criticality, sensitivity, inherent and residual risk along with business impact.	No Exceptions Noted
CC-3.2.3	Identified risks are rated using a risk evaluation process and ratings are reviewed by management annually at the Monthly Management Meeting.	Inspected meeting minutes from the Manager Meetings to determine that risks were rated using a risk evaluation process and ratings and were reviewed by management annually.	No Exceptions Noted
CC-3.2.4	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted

CC-3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.3.1	At the Monthly Manager Meetings, management evaluates the need for changes and re-alignment of the organization structure and reporting.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that needs for changes and re-alignment of the organization structure and reporting were discussed in the Monthly Manager Meetings.	No Exceptions Noted
CC-3.3.2	At Monthly Manager Meetings, the need for additional resources and skills are discussed in order to achieve business objectives.	Inspected meeting minutes from Monthly Manager Meeting for a selection of months to determine that needs for additional resources and skills were discussed in the Monthly Manager Meetings.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.3.3	Identified risks are rated using a risk evaluation process and ratings are reviewed by management annually at the Monthly Management Meeting.	Inspected meeting minutes from the Manager Meetings to determine that risks were rated using a risk evaluation process and ratings and were reviewed by management annually.	No Exceptions Noted
CC-3.3.4	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted
CC-3.3.5	At the Monthly Manager Meetings, management evaluates the detail graphs and spreadsheets about the business operations and performances.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that management evaluated the detail graphs and spreadsheets about the business operations in the Monthly Manager Meetings.	No Exceptions Noted

CC-3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.4.1	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.	<p>Inspected the risk assessment results to determine that changes to infrastructure, data, software, and procedures were documented.</p> <p>Inquired of management to determine whether there was charge request created due to ongoing risk assessment procedures.</p>	<p>No change request was created due to ongoing risk assessment procedures.</p> <p>As a result, no testing of operating effectiveness was performed.</p>

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-3.4.2	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted

CC-4.0 Monitoring Activities			
CC-4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-4.1.1	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted
CC-4.1.2	Monitoring alerts from the independent third party are reviewed by Management.	<p>Inspected an example monitoring alert to determine they were reviewed by Management.</p> <p>Inspected the executed contract with the third party to determine that DriveSavers had an agreement with the third-party provide to monitor DriveSavers' network.</p>	<p>Exception Noted.</p> <p>DriveSavers did not perform reviews for alerts from the independent third party.</p>
CC-4.1.3	Personnel follow defined protocols for escalating reported events.	<p>Inspected information security incident response procedure to determine that protocols existed for escalating for reported events.</p> <p>Inspected the incident recovery form and the call log for the one incident in the period to determine personnel followed defined protocols for escalating a reported event.</p>	No Exceptions Noted

CC-4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-4.2.1	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted

CC-5.0 Control Activities			
CC-5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-5.1.1	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted
CC-5.1.2	Internal and external vulnerability scans are performed annually by an independent third party. The reports from the scans are reviewed by management.	Inspected the vulnerabilities scan reports to determine that internal and external scans were performed. Inspected vulnerability scan review tickets to determine that internal and external scans were reviewed by management.	No Exceptions Noted

CC-5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-5.2.1	Internal and external vulnerability scans are performed annually by an independent third party. The reports from the scans are reviewed by management.	Inspected the vulnerabilities scan reports to determine that internal and external scans were performed. Inspected vulnerability scan review tickets to determine that internal and external scans were reviewed by management.	No Exceptions Noted
CC-5.2.2	At the Monthly Manager Meeting, Management evaluates the effectiveness of the controls on an annual basis.	Inspected meeting minutes from the Monthly Manager Meetings to determine that effectiveness of the controls was evaluated.	No Exceptions Noted

CC-5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-5.3.1	DriveSavers conducts an annual review of all security policies and procedures.	Inspected information security policies to determine that an annual review was performed.	Exception Noted. There was no annual review of all security policies and procedures.

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-5.3.2	Personnel are required to read and accept the code of conduct upon their hire and to formally re-affirm them annually thereafter.	<p>Inspected acknowledgement forms for a selection of new hires during the reporting period to determine that employees read and accepted the code of conduct.</p> <p>Inspected annual acknowledgement forms for a selection of existing employees to determine that employees read and accepted the code of conduct.</p> <p>Inspected DriveSavers' Acceptable Use Policy to determine that Code of Conduct was included in the form.</p>	<p>Exception Noted.</p> <p>Six out of ten current employees did not re-affirm on code of conduct during the audit period.</p> <p>One out of two new hires that were selected for testing did not read and accept the code of conduct upon their hire.</p>
CC-5.3.3	Code of conduct outlines sanctions for employee misconduct.	Inspected the Acceptable Use Policy to determine that Acceptable Use Policy outlined sanctions for employee misconduct.	No Exceptions Noted

CC-6.0 Logical and Physical Access Controls			
CC-6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.1.1	Access to DriveSavers network and tools are approved by the IT manager or the chief information security officer.	Inspected request for access documentation for a selection of new access requests to determine that access was approved by the IT manager.	No Exceptions Noted
CC-6.1.2	Every employee has a unique user account name and a password on the domain.	Inspected user listing from the domain to determine that every employee had a unique user account name and a password on the domain.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.1.3	Every employee has a unique user account name and a password to the CRM application.	Inspected user listing from the CRM to determine that every employee had a unique user account name and a password on the CRM application.	No Exceptions Noted
CC-6.1.4	Privilege access to the domain is restricted based on job responsibilities.	Inspected user listing from the domain to determine that privilege access to the domain was restricted based on job responsibilities.	No Exceptions Noted
CC-6.1.5	Privilege access to the CRM application is restricted based on job responsibilities.	Inspected user listing from the CRM application to determine that privilege access to the CRM application was restricted based on job responsibilities.	No Exceptions Noted
CC-6.1.6	External access by employees is permitted through an encrypted virtual private network (VPN) connection using multi-factor authentication to gain access to the domain.	Inspected the user listing to determine that employees used encrypted VPN connections to connect externally. Inspected the VPN-MFA Configurations to determine that employees utilized multi-factor authentication to connect externally.	No Exceptions Noted
CC-6.1.7	DriveSavers performs an annual review of access controls to confirm all personnel require access to perform their job functions. Annual review is performed to verify employees are still active.	Inspected the annual review ticket of access to determine that the annual review was performed.	No Exceptions Noted
CC-6.1.8	On-site access for users must receive approval by management.	Inspected On-site access request for a selection of new hires to determine that access was approved by management.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.1.9	On-site user’s access is logged and monitored by management.	Inspected the access system log to determine that on-site user access was logged and monitored by management.	No Exceptions Noted

CC-6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credent			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.2.1	Employee access to protected resources is created or modified based on an authorized request from management.	Inspected request access documentation for a selection of new hires during the reporting period to determine that access was approved.	No Exceptions Noted
CC-6.2.2	Management approval to add, change, or remove access to a user account (i.e., employee, temporary employee, and/or contractor) is required. The user account access is consistent with the level required to perform the daily job duties.	<p>Inspected request access documentation for a selection of new hires during the reporting period to determine that access was approved.</p> <p>Inspected request access documentation for a selection of terminations to determine that access was removed.</p> <p>Inspected the current AD listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p> <p>Inspected the current CRM listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p>	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.2.3	Password settings have been configured to comply with industry best practice standards that include complex passwords, a sufficient minimum number of password characters, invalid login restriction, and automatic change password after a set time. Any exception requires a valid business case and documented management approval.	<p>Inspected password configuration to determine that settings were configured to comply with DriveSavers’ policy.</p> <p>Inquired of management to determine that no exceptions existed during the audit period.</p>	<p>No known exception to password settings were noted.</p> <p>As a result, no testing of operating effectiveness was performed.</p>
CC-6.2.4	Human resources send notification of a terminated employee for whose access is to be removed. The notification is used to remove physical and logical access.	<p>Inspected termination ticket documentation for a selection of terminated employees to determine that physical and logical access was removed after notification from HR.</p> <p>Inspected the current AD listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p> <p>Inspected the current CRM listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p>	No Exceptions Noted
CC-6.2.5	Generic, default, application / system and shared user IDs have had their default passwords changed from the initial passwords.	<p>Inspected the application listing to determine that generic, default, application / system and shared user IDs did not exist.</p> <p>Inspected the Active Directory listing to determine that that generic, default, application / system and shared user IDs did not exist.</p>	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.2.6	Known exceptions to access security segregation of duties require a business reason and documented management approval. Review of the known exceptions is performed periodically.	Inquired of management to determine whether known exceptions to access security segregation of duties existed.	No known exceptions were noted. As a result, no testing of operating effectiveness was performed.
CC-6.2.7	Security policy requires password files are encrypted, as needed. Any exception requires a valid business case and documented management approval.	Inspected the security policy to determine that password files were required to be encrypted.	No Exceptions Noted

CC-6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.3.1	Employee access to protected resources is created or modified based on an authorized request from management.	Inspected request access documentation for a selection of new hires during the reporting period to determine that access was approved.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.3.2	Management approval to add, change, or remove access to a user account (i.e., employee, temporary employee, and/or contractor) is required. The user account access is consistent with the level required to perform the daily job duties.	Inspected request access documentation for a selection of new hires during the reporting period to determine that access was approved. Inspected request access documentation for a selection of terminations to determine that access was removed. Inspected the current AD listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed. Inspected the current CRM listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.3.3	Human resources send notification of a terminated employee for whose access is to be removed. The notification is used to remove physical and logical access.	<p>Inspected termination ticket documentation for a selection of terminated employees to determine that physical and logical access was removed after notification from HR.</p> <p>Inspected the current AD listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p> <p>Inspected the current CRM listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p>	No Exceptions Noted
CC-6.3.4	Known exceptions to access security segregation of duties require a business reason and documented management approval. Review of the known exceptions is performed periodically.	Inquired of management to determine whether known exceptions to access security segregation of duties existed.	<p>No known exceptions to access security segregation of duties were noted.</p> <p>As a result, no testing of operating effectiveness was performed.</p>
CC-6.3.5	Periodic access review of employee's access is performed to verify employee is still active and access is restricted based on job functions.	Inspected access review tickets to determine that an annual access review of employee access was performed.	No Exceptions Noted

CC-6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.4.1	ID cards initially provide access only to nonsensitive areas.	Inspected the default settings of an ID cards to determine that access was granted only to nonsensitive areas.	No Exceptions Noted
CC-6.4.2	Access to sensitive areas is added to ID cards by the physical security director based on a request for access approved by the owner of the sensitive area.	Inspected access request for a selection of sensitive access requests during the reporting period to determine that access to sensitive areas was approved.	No Exceptions Noted
CC-6.4.3	Visitors must be signed in by an employee before access to high security areas is granted.	Inspected the visitor log report to determine that visitor must be signed in by an employee before access to high security areas.	No Exceptions Noted
CC-6.4.4	Visitor stickers are used for identification purposes only and do not permit access to any secured areas of the facility.	Inspected visitor pass image to determine that visitor stickers are used for identification purposed only and do not permit access to any secured areas of the facility.	No Exceptions Noted
CC-6.4.5	All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.	Inspected the visitor log report to determine that visitor must be signed in by an employee before access to high security areas.	No Exceptions Noted
CC-6.4.6	Notification of physical access to the facility by visitors is send to all employees.	Inspected a notification of visitor to facility to determine that notification was send to all employees.	No Exceptions Noted
CC-6.4.7	Physical access to sensitive areas of the facility is review by management on a periodic basis.	Inspected the annual review of physical access to sensitive areas to determine that physical access to sensitive areas of the facility was review by management on a monthly basis.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.4.8	All access badges are collected and disabled as part of the exiting process.	Inspected access badges access and cards for a selection of terminated employees to determine that access badges were collected as part of the exiting process.	No Exceptions Noted
CC-6.4.9	Card based access system logs all attempts to enter the facility.	<p>Inspected the security logs to determine that card-based access system logged all attempts to enter the facility with the attempt of a valid access card scanned.</p> <p>Inspected the security logs to determine that card-based access system logged all attempts to enter the facility with the attempt of an invalid access card scanned.</p>	No Exceptions Noted

CC-6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.5.1	Human resources send notification of a terminated employee for whose access is to be removed. The notification is used to remove physical and logical access.	<p>Inspected termination ticket documentation for a selection of terminated employees to determine that physical and logical access was removed after notification from HR.</p> <p>Inspected the current AD listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p> <p>Inspected the current CRM listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.</p>	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.5.2	Management approval to add, change, or remove access to a user account (i.e., employee, temporary employee, and/or contractor) is required. The user account access is consistent with the level required to perform the daily job duties.	Inspected request access documentation for a selection of new hires during the reporting period to determine that access was approved. Inspected request access documentation for a selection of terminations to determine that access was removed. Inspected the current AD listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed. Inspected the current CRM listing for a selection of terminations during the reporting period to determine that terminated accounts access was removed.	No Exceptions Noted
CC-6.5.3	All access badges are collected and disabled as part of the exiting process.	Inspected access badges access and cards for a selection of terminated employees to determine that access badges were collected as part of the exiting process.	No Exceptions Noted

CC-6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.6.1	External access by employees is permitted through an encrypted virtual private network (VPN) connection using multi-factor authentication to gain access to the domain.	Inspected the user listing to determine that employees used encrypted VPN connections to connect externally. Inspected the VPN-MFA Configurations to determine that employees utilized multi-factor authentication to connect externally.	No Exceptions Noted
CC-6.6.2	External points of connectivity are protected by a firewall complex.	Inspected the network diagram to determine that external points of connectivity were protected by a firewall complex.	No Exceptions Noted

CC-6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.7.1	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks.	Inspected Cisco VPN configurations to determine that encryption was used for defined points of connectivity.	No Exceptions Noted
CC-6.7.2	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted.	Inspected security policy to determine that the transmission of sensitive information over the Internet or other public communication paths was prohibited unless it was encrypted.	No Exceptions Noted
CC-6.7.3	Backup media are encrypted during creation.	Inspected backup media tool configuration to determine backup media were encrypted during creation.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.7.4	Policies include encryption requirements based on data classification.	Inspected security policy to determine that encryption requirements were based on data classification.	No Exceptions Noted
CC-6.7.5	Storage for laptops is encrypted.	Inspected encryption settings for a selection of laptops to determine that laptops were encrypted.	No Exceptions Noted

CC-6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-6.8.1	Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected the antivirus software on all workstations, laptops, and servers to determine that antivirus software was installed.	No Exceptions Noted
CC-6.8.2	Antivirus software is configured to receive an updated virus signatures at least daily.	Inspected the antivirus configuration to determine that antivirus signatures were updated daily.	No Exceptions Noted
CC-6.8.3	Spam filter software is implemented to prevent system vulnerabilities and malicious code.	Inspected the filter software configuration to determine that spam filter software was implemented to prevent system vulnerabilities and malicious code.	No Exceptions Noted

CC-7.0 System Operations			
CC-7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-7.1.1	Internal and external vulnerability scans are performed annually by an independent third party. The reports from the scans are reviewed by management.	<p>Inspected the vulnerabilities scan reports to determine that internal and external scans were performed.</p> <p>Inspected vulnerability scan review tickets to determine that internal and external scans were reviewed by management.</p>	No Exceptions Noted
CC-7.1.2	Monitoring alerts from the independent third party are reviewed by Management.	<p>Inspected an example monitoring alert to determine they were reviewed by Management.</p> <p>Inspected the executed contract with the third party to determine that DriveSavers had an agreement with the third-party provide to monitor DriveSavers’ network.</p>	<p>Exception Noted.</p> <p>DriveSavers did not perform reviews for alerts from the independent third party.</p>
CC-7.1.3	Antivirus software is installed on workstations, laptops, and servers supporting such software.	Inspected the antivirus software on all workstations, laptops, and servers to determine that antivirus software was installed.	No Exceptions Noted
CC-7.1.4	At the Monthly Manager Meetings, management discuss the monthly statistics from the IT service provider.	Inspected meeting minutes from the Monthly Manager Meeting for a selection of months to determine that the monthly statistics from the IT service provider were discussed in the Monthly Manager Meetings.	No Exceptions Noted

CC-7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-7.2.1	Procedures documents for problem management processes, which include responsibility for reporting problems (and the process for doing so).	Inspected the procedures to determine that procedures outlined the process for problem management, which included responsibility for reporting problems.	No Exceptions Noted
CC-7.2.2	Users are required to provide proper identification prior to password reset.	Inspected all password resets during the reporting period to determine that users were required to provide proper identification prior to password reset.	No Exceptions Noted
CC-7.2.3	Backup frequency (e.g., daily, weekly, and monthly) and type (e.g., full or incremental) of backup is performed using an automated system.	Inspected backup automated system to determine that backup frequency and type of backup was performed using an automated system.	No Exceptions Noted
CC-7.2.4	Backup logs are monitored to ensure the completeness of the backup process.	Inspected the backup notification email to determine that backup logs were monitored to show completeness of the backup process.	No Exceptions Noted

CC-7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-7.3.1	Operations personnel follow defined protocols for evaluating reported events.	<p>Inspected the procedures to determine that procedures defined protocols for evaluating reported events.</p> <p>Inspected the incident recovery form and the call log for the one incident in the period to determine personnel followed defined protocols for escalating a reported event.</p>	No Exceptions Noted
CC-7.3.2	Resolution of security events (incidents or problems) is reviewed at the monthly management meeting.	Inspected the minutes of the management meetings for a selection of months to determine that resolution of security events was reviewed at the monthly management meeting.	No Exceptions Noted
CC-7.3.3	Code of conduct outlines sanctions for employee misconduct.	Inspected the Acceptable Use Policy to determine that Acceptable Use Policy outlined sanctions for employee misconduct.	No Exceptions Noted
CC-7.3.4	Alerts from the system monitoring tool are sent to various members of the security group when a criterion is met.	<p>Inspected an alert from the system monitoring tool to determine alerts from the system monitoring tool were sent.</p> <p>Inspected the monitoring tool configurations to determine alerts were sent to various members of the security group when a criterion was met.</p>	No Exceptions Noted

CC-7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-7.4.1	Operations personnel follow defined protocols for evaluating reported events.	<p>Inspected the procedures to determine that procedures defined protocols for evaluating reported events.</p> <p>Inspected the incident recovery form and the call log for the one incident in the period to determine personnel followed defined protocols for escalating a reported event.</p>	No Exceptions Noted
CC-7.4.2	External users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	Inspected the incident recovery form and the call log for the one incident in the period to determine external users were informed of incidents in a timely manner and advised of corrective measure to be taken on their part.	No Exceptions Noted

CC-7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-7.5.1	Business recovery plan is tested annually, and results are documented in a memo.	<p>Inspected the operating meeting notes to determine that recovery plan was tested annually, and results were documented.</p> <p>Inspected generator log to determine that the generator was tested as part of the Business Continuity Plan.</p>	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-7.5.2	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.	Inspected the ISP to determine that root cause analysis was required to be prepared and to be reviewed by operations management. Inquired of management to determine whether there were any high severity incidents that required root cause analysis.	No high severity incident occurred. As a result, no testing of operating effectiveness was performed.

CC-8.0 Change Management			
CC-8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-8.1.1	Change requests must be reviewed and approved by the management. Changes are prioritized by management.	Inspected ticket information for a selection of system changes during the reporting period to determine change requests were reviewed, approved, and prioritized by management.	No Exceptions Noted
CC-8.1.2	Change requests are logged in the ticketing system and tracked through to implementation.	Inspected ticket information for a selection of system changes during the reporting period to determine that change requests were logged in the ticketing system and tracked through to implementation.	No Exceptions Noted

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-8.1.3	Change installation / implementation plans are documented, tested, and approved.	Inspected ticket information for a selection of system changes during the reporting period to determine that changes installation / implementation plans were documented, tested, and approved.	No Exceptions Noted
CC-8.1.4	Changes are reviewed and approved by management prior to implementation.	Inspected ticket information for a selection of system changes during the reporting period to determine that changes were reviewed and approved by management prior to implementation.	No Exceptions Noted
CC-8.1.5	Changes are moved into production only by authorized individuals once approval of tests and implementation plans are obtained.	Inspected ticket information for a selection of system changes during the reporting period to determine that changes were moved into production only by authorized individuals once approval of tests and implementation plans were obtained.	No Exceptions Noted
CC-8.1.6	Backout plans are established for each implementation if the event of a failure.	Inspected ticket information for a selection of system changes during the reporting period to determine that back out plans were established for each implementation in the event of a failure.	No Exceptions Noted
CC-8.1.7	On emergency changes, associated documentation and approvals are required after the change has been implemented.	Inquired of management to determine whether any emergency change occurred during the reporting period.	No emergency changes occurred during the reporting period. As a result, no testing of operating effectiveness was performed.

CC-9.0 Risk Mitigation			
CC-9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-9.1.1	An assessment of DriveSavers’ risks is performed on an annual basis, and documented procedures, processes and controls for reducing the identified risks.	<p>Inspected the annual risk assessment to determine that the assessment was performed on an annual basis.</p> <p>Inspected IS Policies to determine that procedures, processes and controls were documented for reducing the identified risks.</p>	No Exceptions Noted
CC-9.1.2	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.	<p>Inspected the risk assessment results to determine that changes to infrastructure, data, software, and procedures were documented.</p> <p>Inquired of management to determine whether there was charge request created due to ongoing risk assessment procedures.</p>	<p>No change request was created due to ongoing risk assessment procedures.</p> <p>As a result, no testing of operating effectiveness was performed.</p>
CC-9.1.3	For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.	<p>Inspected the ISP to determine that root cause analysis was required to be prepare and to be reviewed by operations management.</p> <p>Inquired of management to determine whether there were any high severity incidents that required root cause analysis.</p>	<p>No high severity incident occurred.</p> <p>As a result, no testing of operating effectiveness was performed.</p>

	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-9.1.4	For items assessed, the risk assessment includes identification of business criticality; data sensitivity; relevant threats assessed; inherent and residual risk for each threat assessed; and identification of relevant business impact areas for each threat (financial, legal, compliance, reputation, and operations).	Inspected the annual risk assessment to determine that threats were assessed by criticality, sensitivity, inherent and residual risk along with business impact.	No Exceptions Noted

CC-9.2 The entity assesses and manages risks associated with vendors and business partners.			
	Controls Specified by DriveSavers	Test(s) of Controls Performed by CLA	Results of Test(s)
CC-9.2.1	Vendor due diligence documentation is collected on an annual basis to evaluate the managed services provider(s) ability to support the organization.	Inspected due diligence documentation collected from the managed service provider to determine that the managed service provider was evaluated.	No Exceptions Noted

V. Other Information Provided by DriveSavers Data Recovery, Inc. That Is Not Covered by the Service Auditors' Report

Management Response to All Comments

Due to the tragic loss of a longstanding and critical employee of our SOC II controls and procedures during this audit period, there were controls that didn't get the proper attention. It has taken time to fully implement with new personnel how to continue to perform controls to properly protect the customers, our personnel and the company by fully understanding and performing all duties set out in the controls set by DriveSavers.