



Managed Services | IT Consulting | Data Center

GENERAL CONTROLS SUPPORTING THE DATA CENTER AND MANAGED SERVICES

SOC 2 - Type II Audit Report

*Independent Service Auditor's Report
on Controls Placed in Operation
Relevant to the Trust Services Categories
of Security, Availability, and Confidentiality*

For the Period June 1, 2019 to May 31, 2020



INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	ASSERTIONS BY THE SERVICE ORGANIZATION'S MANAGEMENT	5
SECTION 3	DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM	7
	OVERVIEW OF OPERATIONS	8
	Company Background	8
	Description of Services Provided	8
	CONTROL ENVIRONMENT	13
	Integrity and Ethical Values	13
	Commitment to Competence	14
	Board of Directors' Participation	14
	Management's Philosophy and Operating Style	14
	Organization Structure and Assignment of Authority and Responsibility	15
	Human Resource Policies and Practices	15
	RISK ASSESSMENT	17
	CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES	19
	MONITORING	19
	INFORMATION AND COMMUNICATION SYSTEMS	21
	Information Systems	21
	Communication Systems	21
	COMPLEMENTARY CONTROLS	22
SECTION 4	TESTING MATRICES	24
	MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY	25
	Control Environment	25
	Communication and Information	34
	Risk Assessment	43
	Monitoring Activities	49
	Control Activities	54
	Logical and Physical Access Controls	60
	System Operations	76
	Change Management	84
	Risk Mitigation	89
	MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY	92
	MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY	98

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

**Independent Service Auditor's Report on a Description of a Service Organization's System
and the Suitability of the Design and Operating Effectiveness of Controls
Relevant to Security, Availability, and Confidentiality**

To: DesignDATA,

Scope

We have examined DesignDATA's (designDATA) accompanying description of its data center and managed services and systems found in Section 3 titled "Description of the Service Organization's System Provided by designDATA Management" (description) throughout the period June 1, 2019 to May 31, 2020 based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2019 to May 31, 2020, to provide reasonable assurance that designDATA's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

designDATA uses various third party data centers (subservice organizations) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at designDATA, to achieve designDATA's service commitments and system requirements based on the applicable trust services criteria. The description presents designDATA's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of designDATA's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

designDATA 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 designDATA's service commitments and system requirements were achieved. In Section 2, designDATA has provided its assertion titled "Assertions by the Service Organization's Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. designDATA 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 Auditor's 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 opinion.

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

- obtaining an understanding of the system and the service 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 services 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 included 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 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 or 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 4, titled "Testing Matrices" of this report.

Opinion

In our opinion, in all material respects —

- a. the description presents designDATA's data center and managed services and systems that was designed and implemented throughout the period June 1, 2019 to May 31, 2020 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period June 1, 2019 to May 31, 2020 to provide reasonable assurance that designDATA'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 designDATA's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period June 1, 2019 to May 31, 2020 to provide reasonable assurance that designDATA'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 designDATA's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of designDATA; user entities of designDATA's data center and managed services and systems during some or all of the period June 1, 2019 to May 31, 2020; business partners of designDATA subject to risks arising from interactions with the data center and managed services and systems; 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 the specified parties.

The Moore Group CPA, LLC

Nashua, NH
June 10, 2020

SECTION 2

**ASSERTIONS BY THE
SERVICE ORGANIZATION'S MANAGEMENT**

MANAGEMENT ASSERTION OF DESIGNDATA

The Moore Group CPA, LLC
Nashua, NH 03060

We have prepared the accompanying description of designDATA's (designDATA) data center and managed services and systems titled "Description of the Service Organization's System Provided by designDATA Management" throughout the period June 1, 2019 to May 31, 2020 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (description criteria). The description is intended to provide report users with information about the data center and managed services and systems that may be useful when assessing the risks arising from interactions with designDATA's system, particularly information about system controls that designDATA 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, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

designDATA uses various third party data centers (subservice organizations) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at designDATA, to achieve designDATA's service commitments and system requirements based on the applicable trust services criteria. The description presents designDATA's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of designDATA's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

- 1) The description presents designDATA's data center and managed services and systems that was designed and implemented throughout the period June 1, 2019 to May 31, 2020 in accordance with the description criteria.
- 2) The controls stated in the description were suitably designed throughout the period June 1, 2019 to May 31, 2020 to provide reasonable assurance that designDATA'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 designDATA's controls throughout that period.
- 3) The controls stated in the description operated effectively throughout the period June 1, 2019 to May 31, 2020 to provide reasonable assurance that designDATA'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 designDATA's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY DESIGNDATA MANAGEMENT

DESCRIPTION OF CONTROLS PLACED IN OPERATION

OVERVIEW OF OPERATIONS

Company Background

Founded in 1979, designDATA is a leading IT services company serving the Washington, DC metropolitan area. The company focuses on three lines of business:

- Data Center – A top-of-the-line Tier 4 facility providing three services to designDATA: vHOST Cloud Servers, co-location of customer owned equipment, and data replication services for the purposes of disaster recovery and business continuity.
- Managed Services / Outsourced IT – The day-to-day network administration duties, 24/7 monitoring, and helpdesk services for staff, bundled into a predictable monthly fee.
- IT Consulting – This group provides IT assessments, strategic planning, business process re-engineering, disaster recovery and business continuity planning, database system selection, PCI compliance, data center initiatives, and web strategies.

designDATA's staff of over 80 technology professionals works to ensure that their technology services are planned, implemented and managed to align with their client's business objectives.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the description of services and the five components described below: infrastructure, software, people, procedures and data.

Description of Services Provided

The scope of this audit includes the Data Center and Managed Services of designDATA which includes, but is not limited to, the following:

Data Center Services

Co-Locating in designDATA's data center offers several distinct advantages over traditional premise-based server rooms such as:

- A physical location outside of the immediate metropolitan area
- High level of premise security including 24x7 manned security, man traps, and biometric scanning equipment
- Private caged equipment
- Multiple divergent internet carriers for redundancy
- Redundant power, battery backup, and generator power
- Redundant cooling and environmental controls.

designDATA provides customers with a wide range of options intended to give clients flexibility in choosing their data center needs. These datacenter options include:

- Co-Location Options – With this option, customer-owned server equipment is physically located in designDATA's tier-one data center.
- vHost – designDATA manages a server farm of redundant enterprise hardware, running private, secured, dedicated Application servers, with a 99.99% service level agreement.
- Fiber Optic Connectivity – designDATA, via a network of local metropolitan based carriers, lights fiber optic lines from customer networks directly to the designDATA datacenter in Sterling, VA. These connections connect at interface speeds of 100mb, 1Gb, or 10 Gb per second.
- Metro Ethernet - vHost and Co-Location customers can utilize designDATA's network of EFM (Ethernet First Mile) providers to light high-speed metro Ethernet fiber.
- Disaster Recovery - designDATA customers electing to manage equipment in their own server room may choose to leverage the data center for disaster recovery purposes.
- Data Backup - Replication of customer data from their server room to the designDATA data center.

Managed Services

Managed Services can be broadly defined as transferring the day-to-day administration of a client company's distributed computer systems to designDATA. Engaging designDATA's Managed Services team is like staffing an organization with a CIO, Network Administrators, Security and Communications Engineers, a Helpdesk Engineering team, a purchasing department and a suite of management tools and processes that have normally been available to only large organizations.

designDATA's Managed Services includes, but is not limited to, the following at a predictable monthly fee:

- A dedicated team of senior network engineers assigned for each client account
- Unlimited helpdesk services
- Monitoring of client servers 24x7
- Patching of client servers and desktop computer systems
- On-site service as required or prescheduled visits
- Backup of client data to a secure tier-4 datacenter
- Managed firewall and network security services
- Initial systems assessment and documentation
- Monthly system health reports
- Periodic CIO strategy sessions.

The components of the system used to provide the services are as follows:

Infrastructure

Subservice Organizations - designDATA utilizes a secure third party datacenter known as Cyxtera, located in Washington, DC. This data center continues to provide co-location services to top tier customers for critical production servers and systems. Cyxtera had SOC 1 Type II and SOC 2 Type II audits completed for the review period of July 1, 2018 to June 30, 2019. The scope of this audit does not include the controls of Cyxtera.

To further provide top tier data services to their customers, designDATA also utilizes a secure third party data center known as ByteGrid Holdings LLC ("BYTEGRID"), located in Silver Spring, Maryland. This data center continues to provide co-location services to top tier customers for critical production servers and systems. BYTEGRID had a SOC 2 Type 2 audit completed for the review period of January 1, 2018 to December 31, 2018. The scope of this audit does not include the controls of BYTEGRID.

designDATA's main corporate office is in Gaithersburg, Maryland. A proximity card security system is utilized by designDATA. Environmental controls include but are not limited to fire detection and wet pipe sprinkler systems throughout the facility. UPS systems provide power in the event of disruption of the main power feed, allowing for gradual, safe shutdown of critical computer systems.

Redundant architecture is in place, including:

- Redundant servers for critical systems
- Firewalls configured in an active-passive configuration
- Switches
- Network interface cards (NICs)
- Power supplies
- RAID storage.

Servers and workstations utilize anti-virus endpoint protection, which is kept properly updated and conducts routine scans. Patches for critical production servers are updated manually to ensure adequate testing and that no production interference will result. Workstations are automatically updated.

Software

A combination of custom developed and commercial applications are utilized to support the data center and managed services provided to user organizations. The applications run on Windows Server Operating Systems, VMWare high availability clusters, and storage area networks (SANs) with commercial databases to support the applications.

People

designDATA is led by its President and CEO, Matthew Ruck, and executives in the departmental areas of Technology, Finance, and Customer Service. designDATA's organization structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

In the Control Environment section of this report, additional information is described related to organizational controls implemented at designDATA. These organizational controls are intended to serve as the internal foundation from providing services to its customers.

Procedures

designDATA has implemented processes and procedures to support the operations and controls over the services and systems provided to its customers. Specific examples of the relevant procedures include, but are not limited to, the following:

- Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.
- Security policies are in place to guide personnel regarding physical and information security practices.
- Policies and procedures are in place for identifying the system security requirements of authorized users.
- Third party enterprise monitoring applications are used to monitor and record performance criteria for critical designDATA server and network equipment.
- An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.
- Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.
- Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.
- Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.
- designDATA IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.
- Firewall systems are in place to screen data flow between external parties and the designDATA network.
- designDATA actively utilizes the following firewall features for protection at the perimeter of the network and between network segments:
 - Stateful packet inspection
 - IPsec / Remote Ethernet Device (RED) site-to-site tunnels
 - TLS client-based VPN
 - Intrusion Detection and Prevention
 - Advance Threat Protection
 - Logging and
 - Reporting.
- Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.
- Users are required to authenticate via a unique user ID and password before being granted access to designDATA internal network domain.
- Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.
- Third party antivirus software is installed on all designDATA servers (endpoint protection).
- Management periodically performs internal security assessments, including reviews of server logs and other critical items.
- Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.
- Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.

Data

Access to data is limited to authorized personnel in accordance with designDATA's system security policies. designDATA is also responsible for the overall availability of data, including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving problems.

A third party automated backup application (Veeam) is utilized to perform scheduled system image-based disk-to-disk backups. This results in multiple copies of production data, including:

1. Production data
2. Backup copy on Exagrid appliance
3. Replicated copy at redundant data center
4. Monthly copy to tape is also made, which is stored with AES 256 bit encryption.

Controls in place specific to the data responsibilities of designDATA include, but are not limited to, the following:

- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Firewall systems are in place to screen data flow between external parties and the designDATA network.
- designDATA actively utilizes the following firewall features for protection at the perimeter of the network and between network segments:
 - Stateful packet inspection
 - IPsec / Remote Ethernet Device (RED) site-to-site tunnels
 - TLS client-based VPN
 - Intrusion Detection and Prevention
 - Advance Threat Protection
 - Logging and
 - Reporting.
- Policies and procedures are in place to guide personnel regarding sharing information with third parties.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of designDATA's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of designDATA's ethical and behavioral standards, how they are communicated, and how they are reinforced in daily practice.

These standards include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, and by personal example.

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

- designDATA maintains an **employee handbook**, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Policies and procedures require that new employees sign an **employee handbook acknowledgment form** indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.
- Employees must sign a **confidentiality and non-disclosure agreement** to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive **background checks** are performed by an independent third party for certain positions as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for certain positions within designDATA.
- *Contract employees (1099)* must sign a **confidentiality and non-disclosure agreement** to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive **background checks** are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- Management maintains **insurance coverage** to protect against dishonest acts that may be committed by personnel.

Commitment to Competence

designDATA's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. designDATA's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into **written position requirements** that delineate employee responsibilities and authority.
- Roles and responsibilities for company personnel **to interact with and monitor the activities of external third party information technology vendors** are defined in written job descriptions and communicated to personnel.
- Management utilizes **skills assessment testing** for certain positions during the hiring process.
- Management has developed a **formal training and development program** for employees. This includes:
 - **Initial** training with peers and supervisors in the period immediately after hire.
 - **Ongoing training** to maintain and enhance the skill level of personnel on an as-needed basis.
- Management encourages employees to complete and continue **formal education** and technical certification programs.
- Management-approved **professional development expenses** incurred by the employees are paid by designDATA.
- Employees undergo an **annual performance review** which includes discussions related to their performance related to internal control responsibilities such as data and systems security. A formal evaluation is prepared and is maintained in the employee's HR file.
- designDATA utilizes a **third party financial services** firm to prepare annual tax returns.

Board of Directors' Participation

designDATA's control consciousness is influenced significantly by its Board of Directors participation. The Board of Directors oversees management activities and meets semi-annually to discuss strategic, operational, and compliance issues.

Management's Philosophy and Operating Style

designDATA's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward the data center and managed services, information processing, accounting functions and personnel. Management is periodically briefed on regulatory and industry changes affecting services provided. Management meetings are held on a periodic basis to discuss and monitor operational issues.

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

- Management regularly attends **trade shows**, utilizes **trade and regulatory publications, journals, online news feeds and government sites**, and belongs to **industry associations** to stay current on regulatory compliance or operational trends affecting the services provided.
- Operational meetings are held on a regular basis to **discuss internal control responsibilities (data and system security)** of individuals and performance measurement.
- designDATA utilizes a **third party financial services** firm to prepare annual tax returns.

Organization Structure and Assignment of Authority and Responsibility

designDATA's organization structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. designDATA's management believes that establishing a relevant organization structure includes considering key areas of authority and responsibility and appropriate lines of reporting. designDATA has developed an organization structure suited to its needs. This organization structure is based, in part, on its size and the nature of its activities.

designDATA's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

- **Organizational charts** are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed.
- designDATA's **organizational structure** is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by the CEO.

Human Resource Policies and Practices

designDATA's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- Human Resources management utilizes an **onboarding checklist** to ensure that specific elements of the hiring process are consistently executed. A copy of the onboarding checklist is maintained in the employee file.

- Comprehensive **background checks** are performed by an independent third party for certain positions as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for certain positions within designDATA.
- Comprehensive **background checks** are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- designDATA maintains an **employee handbook**, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Management has developed a **formal training and development program** for employees. This includes:
 - **Initial** training with peers and supervisors in the period immediately after hire.
 - **Ongoing training** to maintain and enhance the skill level of personnel on an as-needed basis.
- Employees undergo an **annual performance review** which includes discussions related to their performance related to internal control responsibilities such as data and systems security. A formal evaluation is prepared and is maintained in the employee's HR file.
- Human Resources management utilizes a **termination checklist** to ensure that specific elements of the termination process are consistently executed. This includes but is not limited to the terminated employee's physical and logical access to company facilities and computer systems. The checklist is retained in the employee files.

RISK ASSESSMENT

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the services and systems. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

Objective Setting

designDATA establishes objectives in order for management to identify potential events affecting their achievement. designDATA has placed into operation a risk management process to help ensure that the chosen control objectives support and align with the organization's mission and are consistent with its risk framework. Objective setting enables management to identify measurement criteria for performance, with focus on success factors.

designDATA has established certain broad categories including:

- **Strategic Objectives** — these pertain to the high level organizational goals and the alignment of those goals to support the overall mission
- **Operations Objectives** — these pertain to effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding of resources against loss
- **Reporting Objectives** — these pertain to the preparation of reliable reporting
- **Compliance Objectives** — these pertain to adherence to laws and regulations to which the entity is subject

Risks Identification

Regardless of whether an objective is stated or implied, an entity's risk-assessment process should consider risks that may occur. It is important that risk identification be comprehensive. designDATA has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user organizations.

Management considers risks that can arise from both external and internal factors including:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives, pressures, and opportunities for employees, as well as employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

The designDATA risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. designDATA senior management oversees risk management ownership, accountability, and is involved in risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards and the likelihood of a threat, to determine the actions to be taken.

Risks Analysis

designDATA's methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities

Control activities are a part of the process by which designDATA strives to achieve its business objectives. designDATA has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

The applicable trust criteria and related control activities are included in Section 4 (the “Testing Matrices”) of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the applicable trust criteria and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of designDATA’s description of controls and systems.

The description of the service auditor’s tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization’s description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

designDATA’s management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, client conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Ongoing and Separate Evaluations of the Control Environment

Monitoring can be done in two ways: through ongoing activities or separate evaluations. The greater the degree and effectiveness of ongoing monitoring, the less the need is for separate evaluations. Management determines the need for separate evaluations by consideration given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring. Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary; to help ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of designDATA's ongoing monitoring activities include the following:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function.
- Communications from external parties and customers corroborate internally generated information or indicate problems.
- Organization structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Training, planning sessions, and other meetings provide important feedback to management on whether controls are effective.
- Personnel are briefed on organizational policy statements and codes of conduct to communicate entity values.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Reporting Deficiencies

Deficiencies in management's internal control system surface from many sources, including designDATA's ongoing monitoring procedures, separate evaluations of the internal control system and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in designDATA's procedures or personnel.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

A combination of custom developed and commercial applications are utilized to support the data center and managed services provided to user organizations. The applications run on Windows Server Operating Systems, VMWare high availability clusters, and storage area networks (SANs) with commercial databases to support the applications.

Redundancy is maintained for components of the data infrastructure, including firewalls, routers, servers and switches. Systems are developed and deployed to enable the addition of bandwidth and server capacity quickly to support customer requirements. External services and internal applications constantly monitor communications, job logs, system performance, and security and send alerts to the operations staff before customers are affected.

Communication Systems

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 a higher level within designDATA. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place at designDATA. Management's communication activities are made electronically, verbally, and through the actions of management.

SUBSERVICE ORGANIZATIONS

The third party data center services provided by the utilized data centers are monitored by designDATA management but are not included in the scope of this audit. The following controls are expected to be implemented by the third party data centers.

SUBSERVICE ORGANIZATION CONTROLS		
Category	Criteria	Applicable Controls
Security	CC6.3 CC6.4	The third party data center has physical access controls in place to <i>restrict access</i> to authorized personnel only.
Security	CC6.5	The third party data center has physical access controls in place to <i>remove access</i> when no longer required.
Security Availability	CC4.1 A1.2	The third party data center is responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by designDATA.
Security	CC8.1	The third party data center is responsible for the general IT controls relevant to its application development and/or change management.
Availability	A1.2	The environmental security and maintenance controls at the third party data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.

COMPLEMENTARY CONTROLS AT USER ORGANIZATIONS

designDATA's services are designed with the assumption that certain controls will be implemented by user organizations. Such controls are called complementary user organization controls. It is not feasible for all of the control objectives related to designDATA's data center and managed services to be solely achieved by designDATA's control procedures. Accordingly, user organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of designDATA.

The following complementary user organization controls should be implemented by user organizations to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user organizations' locations, user organizations' auditors should exercise judgment in selecting and reviewing these complementary user organization controls, which may include:

- User organizations are responsible for understanding and complying with their contractual obligations to designDATA. (CC2.3; CC5.3; CC9.2)
- User organizations are responsible for developing their own disaster recovery and business continuity plans that address their ability to access or utilize designDATA services. (CC5.2; CC 7.2; A1.2; A1.3)
- User organizations are responsible for ensuring that access codes, keys, and other means of accessing designDATA facilities and customer equipment within those facilities are kept in a secure manner and only used by authorized employees. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for ensuring that user IDs and passwords used to access designDATA applications are kept in a secure manner and only used by authorized employees. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for requesting an authorized user ID and password for user organization employees. User organizations are responsible for defining the level of access given to employees and customers. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for requesting the revocation of application access privileges assigned to terminated employees as a component of the employee termination process. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for restricting administrative privileges within the application or systems to authorized personnel and for designating internal personnel who are authorized to request user additions, deletions, and security level changes. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for notifying designDATA of changes made to technical or administrative contact information in a timely manner. (CC6.2)
- User organizations are responsible for understanding and defining data storage requirements. (CC4.1)
- User organizations are responsible for understanding and implementing encryption protocols to protect data during transfer to designDATA. (CC6.6; CC6.7)
- User organizations are responsible for immediately notifying designDATA of any actual or suspected information security breaches, including compromised user accounts and passwords. (CC7.2)
- User organizations are responsible for notifying designDATA of any regulatory issues that may affect the services provided by designDATA. (CC2.3; CC3.2)

COMPLEMENTARY CONTROLS AT SUBSERVICE ORGANIZATIONS

In designing its system, designDATA has contemplated that certain complementary controls would be implemented by its subservice organizations to achieve the applicable criteria included in this report. This section describes the subservice organization's internal controls that, in combination with the controls at designDATA, provide reasonable assurance that designDATA can achieve the applicable criteria included in this report.

The controls below are the responsibility of each subservice organization.

- Subservice Organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and clients is added only for authorized individuals. (CC6.3; CC6.4)
- Subservice Organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and clients is removed when no longer required. (CC6.5)
- Subservice Organizations are responsible for implementing physical access mechanisms to ensure only authorized badge holders can enter the data centers. (CC6.3; CC6.4)
- Subservice Organizations are responsible for ensuring customer-specific areas with the data center can only be accessed by the customer. (CC6.3; CC6.4)
- Subservice Organizations are responsible for providing environmental security and maintenance controls that are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. (A1.2)
- Subservice Organizations are responsible for the general IT controls relevant to its application development and/or change management. (CC8.1)
- Subservice Organizations are responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by designDATA. (CC4.1; A1.2)

SECTION 4
TESTING MATRICES

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1	<p>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</p>	<p>designDATA maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.</p> <p>Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.</p> <p>Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.</p> <p>Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.</p>	<p>Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.</p> <p>Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook.</p> <p>Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.</p> <p>Inspected completed background checks for a judgmental sample of employees hired during the review period to determine that</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Management personnel perform reference checks on all candidates being considered for certain positions within designDATA.</p>	<p>background checks are performed by an independent third party.</p> <p>Inquired of management to determine that management personnel perform reference checks on all candidates being considered for certain positions within designDATA.</p>	<p>No exceptions noted.</p>
		<p><i>Contract employees (1099)</i> must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.</p>	<p>Inspected completed acknowledgment forms for a judgmental sample of <i>contract employees</i> hired during the review period to determine that the <i>contract employees (1099)</i> signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.</p>	<p>No exceptions noted.</p>
		<p>Comprehensive background checks are performed by an independent third party for <i>contract employees (1099)</i> as a component of the hiring process.</p>	<p>Inquired of management to determine that background checks are performed by an independent third party for <i>contract employees (1099)</i> as a component of the hiring process.</p>	<p>No exceptions noted.</p>
		<p>Management maintains insurance coverage to protect against dishonest acts that may be committed by personnel.</p>	<p>Inspected insurance coverage policy declarations page to determine that management maintained insurance coverage to protect against dishonest acts by personnel.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	designDATA utilizes a third party financial services firm to prepare annual tax returns.	Inquired of management to determine that designDATA utilizes a third party financial services firm to prepare annual tax returns.	No exceptions noted.
			Inspected the most recent engagement letter reflecting the engagement of a third party financial services firm to determine that management engages a third party financial services firm to prepare annual tax returns.	No exceptions noted.
		A board of directors oversees management activities.	Inquired of management regarding the board of directors to determine that a board of directors was in place to oversee management activities.	No exceptions noted.
			Inspected the listing of the board of director members to determine that a board of directors was in place.	No exceptions noted.
		The board of directors meets on a semi-annual basis.	Inquired of management to determine that a board of directors meets semi-annually.	No exceptions noted.
		Inspected the most recent BOD meeting agenda to determine that the board of directors meets on a semi-annual basis.	No exceptions noted.	
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position	Inspected a judgmental sample of written job descriptions to determine that management had	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	<p>appropriate authorities and responsibilities in the pursuit of objectives.</p>	<p>requirements that delineate employee responsibilities and authority.</p> <p>Roles and responsibilities for company personnel to interact with and monitor the activities of external third party information technology vendors are defined in written job descriptions and communicated to personnel.</p> <p>Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed.</p> <p>designDATA's organizational structure is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by the CEO.</p>	<p>considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.</p> <p>Inspected a judgmental sample of written job descriptions to determine that written job descriptions contain roles and responsibilities for company personnel to interact with and monitor the activities of external third party information technology vendors.</p> <p>Inquired of management regarding communication of organizational charts to determine that the charts are communicated to employees and updated as needed.</p> <p>Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority and responsibility and are updated as needed.</p> <p>Inquired of management to determine that designDATA's organizational structure is traditional, with clear lines of authority and responsibility, and that autonomy within departments is allowed to a reasonable extent to provide for innovative approaches</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security policies.	to managing the company, with close oversight maintained by the CEO. Inspected the policies and procedures to determine that the entity's policies included procedures regarding training and other resources to support its system security policies.	No exceptions noted.
		Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.	Inspected completed background checks for a judgmental sample of employees hired during the review period to determine that background checks are performed by an independent third party.	No exceptions noted.
		Management personnel perform reference checks on all candidates being considered for certain positions within designDATA.	Inquired of management to determine that management personnel perform reference checks on all candidates being considered for certain positions within designDATA.	No exceptions noted.
		Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements that delineate employee responsibilities and authority.	Inspected a judgmental sample of written job descriptions to determine that management had considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
		Management utilizes skills assessment testing for certain positions during the hiring process.	Inquired of management to determine that management	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Management has developed a formal training and development program for employees. This includes:</p> <ul style="list-style-type: none"> • Initial training with peers and supervisors in the period immediately after hire. • Ongoing training to maintain and enhance the skill level of personnel on an as-needed basis. <p>Management encourages employees to complete and continue formal education and technical certification programs.</p>	<p>utilizes skills assessment testing for certain positions during the hiring process.</p> <p>Inquired of management into initial and ongoing training and development for employees, to determine that a program is in place.</p> <p>Inspected a judgmental sample of company documentation (meeting agendas, assignments) of initial training and development for new employees.</p> <p>Inspected a judgmental sample of documented training programs (meeting agendas, assignments) for tenured employees to determine that ongoing training is utilized for each employee on an as-needed basis beyond the initial hiring training period.</p> <p>Inquired of management into encouragement of employees to pursue formal education and technical certification programs to determine that management encourages employees to complete and continue formal education and technical certification programs.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Management-approved professional development expenses incurred by the employees are paid by designDATA.	Inspected employee handbook for policies related to formal education and technical certification programs, to determine that management encourages employees to continue and complete formal education and technical programs.	No exceptions noted.
		A policy is in place to assign responsibility and accountability for developing and maintaining the entity's security policies, and changes and updates to those policies, to appropriate personnel.	Inspected employee handbook for policies related to expense reimbursement for education and technical certification programs, to determine that management-approved professional development expenses incurred by the employees are paid by designDATA.	No exceptions noted.
		Operational meetings are held on a regular basis to discuss internal control responsibilities (<i>data and system security</i>) of individuals and performance measurement.	Inspected the policies and procedures to determine that responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, were assigned to appropriate personnel. Inquired of management to determine that operational meetings are held on a regular basis to discuss internal control responsibilities (<i>data and system security</i>) of individuals and performance measurement.	No exceptions noted. No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Employees undergo an annual performance review which includes discussions related to their performance related to internal control responsibilities such as data and systems security. A formal evaluation is prepared and is maintained in the employee's HR file.</p> <p>Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed.</p> <p>designDATA's organizational structure is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by the CEO.</p>	<p>Inspected a judgmental sample of annual performance reviews to determine that employees undergo an annual performance review and that a formal evaluation is prepared and is maintained in the employee's HR file.</p> <p>Inquired of management to determine that performance related to internal control responsibilities such as data and systems security was discussed.</p> <p>Inquired of management regarding communication of organizational charts to determine that the charts are communicated to employees and updated as needed.</p> <p>Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority and responsibility and are updated as needed.</p> <p>Inquired of management to determine that designDATA's organizational structure is traditional, with clear lines of authority and responsibility, and that autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			close oversight maintained by the CEO.	

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	<p>A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas:</p> <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. 	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	designDATA has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	Inspected internal processes and procedures to determine that designDATA has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding training and other resources to support its system security policies.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding the handling of exceptions and situations not specifically addressed in its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding the handling of exceptions and situations not specifically addressed in its system security policies.	No exceptions noted.
		Policies and procedures are in place to assign responsibility and accountability for system security.	Inspected the policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system security.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are in place for identifying the system security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system security policies were established.	No exceptions noted.
		Security policies are in place to guide personnel regarding physical and information security practices.	Inspected the policies and procedures manual to determine that security policies were in place to guide personnel regarding physical and information security practices.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.	No exceptions noted.
		Policies and procedures are in place to communicate responsibility and accountability for the entity's confidentiality and related security policies and changes and updates to those policies.	Inspected the policies and procedures to determine that responsibility and accountability for the entity's confidentiality and related security policies and changes and updates to those policies were communicated to entity personnel responsible for implementing them.	No exceptions noted.
		Procedures have been implemented to protect confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	Inspected confidentiality policies and procedures implemented to protect confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are in place to govern critical computer operations activities.	Inspected the policies and procedures to determine that policies and procedures are in place to govern critical computer operations activities.	No exceptions noted.
		New client contracts are approved by designDATA management prior to initiating service. A Service Level Agreement (SLA) is signed by the client and designDATA management.	Inspected a judgmental sample of new client contracts and SLAs formalized during the review period to determine that they are signed off by the client and designDATA management.	No exceptions noted.
		An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.	Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.	No exceptions noted.
		Management has developed designDATA's definition of system downtime and determined acceptance level criteria.	Inspected policies and procedures to determine management has developed designDATA's definition of system downtime and acceptance level criteria.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor and record performance criteria for critical <i>designDATA</i> server and network equipment.	Inspected the Kaseya enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical <i>designDATA</i> server and network equipment.	No exceptions noted.
		A third party enterprise monitoring application is used to monitor and record performance criteria	Inspected the enterprise monitoring application to determine that a third party enterprise monitoring	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>for contracted <i>client</i> server and network equipment.</p> <p>System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.</p> <p>The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via text or email to appropriate support personnel.</p> <p>All designDATA network operations center personnel are equipped with smart phones for use in the network and server monitoring alert process.</p> <p>designDATA provides network operations center personnel on a 24/7/365 basis for server and network performance monitoring.</p>	<p>application is used to monitor performance criteria for contracted client server and network equipment.</p> <p>Inspected the Kaseya metrics tracking reports to determine that system downtime and operations issues were monitored.</p> <p>Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.</p> <p>Observed smart phones of network operations center personnel to determine that network operations center personnel are equipped with smart phones for use in the network and server monitoring alert process.</p> <p>Inquired of management to determine that designDATA network operations center personnel are provided on a 24/7/365 basis for server and network performance monitoring.</p> <p>Observed server and network performance monitoring in network operations center to determine that designDATA provides network operations center personnel on a</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Network diagrams are in place and communicated to appropriate personnel.</p> <p>Documented backup procedures are in place for company systems deemed critical by management, to guide personnel in performing backup system tasks.</p> <p>Documented backup procedures are in place for <i>customer</i> system backups performed by designDATA.</p> <p>Data backups of contracted <i>customer</i> application components and databases are performed according to the timing reflected in the customer contract.</p> <p>designDATA maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.</p> <p>Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it, and understand their</p>	<p>24/7/365 basis for server and network performance monitoring.</p> <p>Inspected network diagrams to determine that network diagrams are in place and communicated to appropriate personnel.</p> <p>Inspected documented backup procedures to determine that documented backup procedures are in place for critical designDATA systems.</p> <p>Inspected documented backup procedures to determine that documented backup procedures are in place for critical customer systems.</p> <p>Inquired of management to determine that data backups of contracted customer application components and databases are performed according to the timing reflected in the customer contract.</p> <p>Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.</p> <p>Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.	determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	
		Policies and procedures are in place to assign responsibility and accountability for system security.	Inspected the policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system security.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures to guide personnel regarding sharing information with third parties.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Procedures have been implemented to protect confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	Inspected confidentiality policies and procedures implemented to protect confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	No exceptions noted.
		Policies and procedures are in place for identifying the system security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system security policies were established.	No exceptions noted.
		New client contracts are approved by designDATA management prior to initiating service. A Service Level Agreement (SLA) is signed by the client and designDATA management.	Inspected a judgmental sample of new client contracts and SLAs formalized during the review period to determine that they are signed off by the client and designDATA management.	No exceptions noted.
		Customers are notified of scheduled system downtime and emergency changes via the company ticketing system or customer portal.	Inspected a judgmental sample of ticketing email notifications to determine that customers are notified of scheduled system downtime and emergency changes.	No exceptions noted.
		Management has developed designDATA's definition of system downtime and determined acceptance level criteria.	Inspected policies and procedures to determine management has developed designDATA's definition of system downtime and acceptance level criteria.	No exceptions noted.
		Prior to collecting personal information of external users, a privacy policy is provided that may include the purpose and use of the personal information, including detailed use, ability to opt-out, enhancement (enrichment),	Inspected policies to determine that if personal information of external users is collected, a privacy policy is provided that may include the purpose and use of the collection of	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		sharing, disclosure, access, security, retention, and disposal of personal information.	their personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, and disposal of personal information.	

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	<p>A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas:</p> <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. 	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2	COSO Principle 7: 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.	<p>Management regularly attends trade shows, utilizes trade and regulatory publications, journals, online news feeds and government sites, and belongs to industry associations to stay current on regulatory compliance or operational trends affecting the services provided.</p> <p>Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.</p> <p>Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.</p> <p>A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas:</p> <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information 	<p>Inspected a judgmental sample of trade show agendas, online sites utilized and publications, and association membership literature to determine that management is periodically briefed on regulatory and industry changes affecting services provided.</p> <p>Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.</p> <p>Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.</p> <p>Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<ul style="list-style-type: none"> • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. <p>Management regularly attends trade shows, utilizes trade and regulatory publications, journals, online news feeds and government sites, and belongs to industry associations to stay current on regulatory compliance or operational trends affecting the services provided.</p> <p>Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.</p>	<p>Inspected a judgmental sample of trade show agendas, online sites utilized and publications, and association membership literature to determine that management is periodically briefed on regulatory and industry changes affecting services provided.</p> <p>Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3	COSO Principle 8: The entity considers the potential for fraud in		Inspected current agreements with third party vendors to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3 rd party vendors.	No exceptions noted.
		designDATA maintains an inventory of spare equipment for most critical network and server systems to help ensure rapid recovery if necessary.	Inspected inventory of spare equipment to determine that designDATA maintains an inventory of spare equipment for most critical network and server systems to help ensure rapid recovery if necessary.	No exceptions noted.
		designDATA maintains redundant servers for critical production applications.	Inquired of management to determine that designDATA maintains redundant servers for critical production applications.	No exceptions noted.
		Redundant architecture is built into server infrastructure, including, but not limited to the: <ul style="list-style-type: none"> • Network interface cards (NICs) • Power supplies • RAID storage. 	Observed redundant system infrastructure and the network configuration documentation to confirm server redundancy for critical production applications.	No exceptions noted.
		A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally	Observed the redundant system infrastructure components to determine that redundant architecture was built into certain aspects of the systems infrastructure.	No exceptions noted.
			Inspected the annual risk assessment documentation to determine that a formal risk	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	<p>assessing risks to the achievement of objectives.</p>	<p>documented in memo form. The risk assessment includes, but is not limited to, the following areas:</p> <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. 	<p>assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.</p>	
CC3.4	<p>COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</p>	<p>A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk</p>	<p>Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		assessment includes, but is not limited to, the following areas: <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. 	risks and mitigation strategies were formally documented.	

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	<p>Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.</p> <p>Management periodically performs internal security assessments, including reviews of server logs and other critical items.</p> <p>Management has developed designDATA's definition of system downtime and determined acceptance level criteria.</p> <p>Third party enterprise monitoring applications are used to monitor and record performance criteria for critical <i>designDATA</i> server and network equipment.</p> <p>A third party enterprise monitoring application is used to monitor and record performance criteria for contracted <i>client</i> server and network equipment.</p>	<p>Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.</p> <p>Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.</p> <p>Inspected policies and procedures to determine management has developed designDATA's definition of system downtime and acceptance level criteria.</p> <p>Inspected the Kaseya enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical designDATA server and network equipment.</p> <p>Inspected the enterprise monitoring application to determine that a third party enterprise monitoring application is used to monitor performance criteria for contracted client server and network equipment.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.</p> <p>The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via text or email to appropriate support personnel.</p> <p>designDATA provides network operations center personnel on a 24/7/365 basis for server and network performance monitoring.</p> <p>Certain network events are logged and maintained for management review. Critical servers have auditing enabled, and for security, system management and network functions. Monthly proactive system health checks are performed by IT staff.</p>	<p>Inspected the Kaseya metrics tracking reports to determine that system downtime and operations issues were monitored.</p> <p>Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.</p> <p>Inquired of management to determine that designDATA network operations center personnel are provided on a 24/7/365 basis for server and network performance monitoring.</p> <p>Observed server and network performance monitoring in network operations center to determine that designDATA provides network operations center personnel on a 24/7/365 basis for server and network performance monitoring.</p> <p>Inspected the network account and local event monitoring configurations, and event logs and monthly health check documentation to determine that certain network events were logged and maintained for management review.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2	COSO Principle 17: 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.		Inspected a judgmental sample of server configurations to determine that critical servers have auditing enabled, and for security, system management and network functions.	No exceptions noted.
		designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers are responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by designDATA.	Inspected the most recent SOC audit reports for the various third party data centers to determine that designDATA utilizes relevant reports provided by the various third party data centers.	No exceptions noted.
		designDATA management reviews the SOC audit reports of the various third party data centers annually and documents the results of the reviews of the SOC audit reports in a memo.	Inquired of management to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.	No exceptions noted.
		Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inspected management’s memo to determine that designDATA management documents the results of the reviews of the SOC reports in a memo. Inspected the policies and procedures manual to determine that the entity’s system security policies and procedures are in place and periodically reviewed by a designated individual or group.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Management has developed designDATA's definition of system downtime and determined acceptance level criteria.</p> <p>Third party enterprise monitoring applications are used to monitor and record performance criteria for critical <i>designDATA</i> server and network equipment.</p> <p>A third party enterprise monitoring application is used to monitor and record performance criteria for contracted <i>client</i> server and network equipment.</p> <p>System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.</p> <p>The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via text or email to appropriate support personnel.</p> <p>Management periodically performs internal security assessments, including reviews of server logs and other critical items.</p>	<p>Inspected policies and procedures to determine management has developed designDATA's definition of system downtime and acceptance level criteria.</p> <p>Inspected the Kaseya enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical designDATA server and network equipment.</p> <p>Inspected the enterprise monitoring application to determine that a third party enterprise monitoring application is used to monitor performance criteria for contracted client server and network equipment.</p> <p>Inspected the Kaseya metrics tracking reports to determine that system downtime and operations issues were monitored.</p> <p>Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.</p> <p>Inspected a judgmental sample of results from internal security assessments performed during the</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Certain network events are logged and maintained for management review. Critical servers have auditing enabled, and for security, system management and network functions. Monthly proactive system health checks are performed by IT staff.</p>	<p>review period to determine that management periodically performs internal security assessments.</p> <p>Inspected the network account and local event monitoring configurations, and event logs and monthly health check documentation to determine that certain network events were logged and maintained for management review.</p> <p>Inspected a judgmental sample of server configurations to determine that critical servers have auditing enabled, and for security, system management and network functions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	<p>Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.</p> <p>Security policies and procedures are in place and periodically reviewed by a designated individual or group.</p> <p>A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas:</p> <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business 	<p>Inspected the policies and procedures manual to determine that the entity’s policies included procedures regarding assessing risks on a periodic basis.</p> <p>Inspected the policies and procedures manual to determine that the entity’s system security policies and procedures are in place and periodically reviewed by a designated individual or group.</p> <p>Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	<p>operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies</p> <ul style="list-style-type: none"> • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. 		
		<p>Management periodically performs internal security assessments, including reviews of server logs and other critical items.</p>	<p>Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.</p>	<p>No exceptions noted.</p>
		<p>Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.</p>	<p>Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.</p>	<p>No exceptions noted.</p>
		<p>Security policies and procedures are in place and periodically reviewed by a designated individual or group.</p>	<p>Inspected the policies and procedures manual to determine that the entity's system security policies and procedures are in place and periodically reviewed by a designated individual or group.</p>	<p>No exceptions noted.</p>
		<p>Management periodically performs internal security assessments, including reviews of server logs and other critical items.</p>	<p>Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Firewall systems are in place to screen data flow between external parties and the designDATA network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.</p> <p>Multiple production firewalls are utilized for redundancy. The firewalls are set up in an active/passive configuration with automatic failover in the event of failure of the primary.</p> <p>Firewall configurations filter internet traffic based on content and destination site address. The configurations include:</p> <ul style="list-style-type: none"> • The firewall performs stateful packet inspection. • Network Address Translation (NAT) services are enabled on all network firewalls to hide internal servers. • Firewall ports are configured to allow only specific types of traffic between 	<p>management periodically performs internal security assessments.</p> <p>Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and designDATA network.</p> <p>Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.</p> <p>Inspected the network diagram to determine that multiple firewalls are setup for redundancy.</p> <p>Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.</p> <p>Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address, and that the firewall performs stateful packet inspection.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>certain destinations. All unused ports on the firewall are blocked.</p> <ul style="list-style-type: none"> • The firewall is configured to deny all traffic that is not specifically authorized in the rule set. <p>designDATA actively utilizes the following firewall features for protection at the perimeter of the network and between network segments:</p> <ul style="list-style-type: none"> • Stateful packet inspection • IPsec / Remote Ethernet Device (RED) site-to-site tunnel • TLS client-based VPN • Intrusion Detection and Prevention • Advance Threat Protection • Logging and • Reporting. 	<p>Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.</p> <p>Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.</p> <p>Inspected the firewall documentation to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.</p> <p>Inspected firewall configurations to determine that designDATA actively utilizes the stated firewall features for protection at the perimeter of the network and between network segments.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	<p>Policies and procedures are in place to govern critical computer operations activities.</p> <p>An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.</p> <p>designDATA's policies and procedures address controls over significant aspects of system operations. Policies and procedures addressed include:</p> <ul style="list-style-type: none"> • security requirements for authorized users • data classification and associated protection, access rights, retention, and destruction requirements • risk assessment • access protection requirements • user provisioning and deprovisioning • responsibility and accountability for security • responsibility and accountability for system changes and maintenance change management • complaint intake and resolution • security and other incidents identification, response, and mitigation • security training • handling of exceptions and situations not specifically addressed in policies 	<p>Inspected the policies and procedures to determine that policies and procedures are in place to govern critical computer operations activities.</p> <p>Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.</p> <p>Inspected the policies and procedures to determine the policies and procedures addressed controls over significant aspects of the system operations.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<ul style="list-style-type: none"> • commitment and requirement identification and compliance measurement • information sharing and disclosure. <p>designDATA's security policies are reviewed and updated annually by senior management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.</p> <p>Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements that delineate employee responsibilities and authority.</p>	<p>Inspected documentation of the annual review and update of the security policies to determine the policies are reviewed annually by senior management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.</p> <p>Inspected a judgmental sample of written job descriptions to determine that management had considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1	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.	<p>Procedures have been implemented related to confidentiality of inputs, data processing, and outputs which are consistent with the documented confidentiality policies.</p> <p>Users are required to authenticate via a unique user ID and password before being granted access to designDATA internal network domain.</p> <p>Internal network domain (default domain) passwords must conform to the following requirements:</p> <ul style="list-style-type: none"> • Enforce password history • Maximum password age • Minimum password length • Complexity requirements. <p>User IDs are locked out (automatically suspended) after a designated number of invalid login attempts within a set time period. The account is then locked out of the system for a set time period, and a notification alert is triggered.</p>	<p>Inspected confidentiality policies and procedures to determine that procedures have been implemented related to confidentiality of inputs, data processing, and outputs which are consistent with the documented confidentiality policies.</p> <p>Inspected the internal network domain authentication process to determine that users are required to authenticate via a unique user ID and password before being granted access to designDATA internal network domain.</p> <p>Inspected the network authentication configurations to determine that network domain passwords must conform to stated requirements.</p> <p>Inspected the password configuration screen to determine that user IDs are locked out after a designated number of invalid login attempts within a set time period, and that the account is then locked out of the system for a set time period, and a notification is triggered.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Production database and application server operating system account policies are controlled by the default domain group policy.</p> <p>Management has segregated specific duties within the internal network domain for administering critical areas such as network administration and database management. Management restricts network domain administration privileges to approved positions only.</p>	<p>Inquired of the network administrator regarding operating system account policies to determine that database and application server operating system account policies were controlled by the default domain group policy.</p> <p>Inspected a judgmental sample of application and database server configurations to determine that the database and application server operating system account policies were controlled by the default domain group policy.</p> <p>Inquired of management to determine that management has authorized specific personnel to administer information security within the internal network domain, and has segregated duties.</p> <p>Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the production environment, and has segregated specific duties within the internal network domain for administering critical areas such as network administration, and database management.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Management has segregated specific duties within the production environment for administering critical areas such as:</p> <ul style="list-style-type: none"> • Network administration • Systems (including Active Directory) administration. <p>Firewall systems are in place to screen data flow between external parties and the designDATA network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.</p> <p>The firewall requires two factor authentication before administrative access to the firewall system is allowed.</p> <p>Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.</p>	<p>Inspected access rights listing to determine that management has segregated specific duties within the production environment for administering critical areas.</p> <p>Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and designDATA network.</p> <p>Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.</p> <p>Observed the network engineer log into the firewall system to determine that the firewall required two factor authentication before administrative access to the firewall system was allowed.</p> <p>Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2	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	The backup application encrypts the backup data for storage utilizing AES 256 bit encryption.	client information, to unauthorized parties. Inspected the control panel encryption settings to determine that the backup application encrypts the backup data for storage.	No exceptions noted.
		Only authorized personnel are granted access rights to recall backup data from the storage site at HQ or from the storage appliance.	Inspected the backup media access rights to determine that only authorized personnel are granted rights to recall backup media from storage.	No exceptions noted.
		Management has a data classification methodology to identify and classify sensitive data in the production environment.	Inquired of management to determine that management has a data classification methodology to identify and classify sensitive data.	No exceptions noted.
		Encryption methods are in place and utilized for sensitive backup data storage.	Inspected encryption configurations to determine that encryption methods are in place and utilized for sensitive backup data storage.	No exceptions noted.
			Inspected encryption policies to determine that encryption methods are in place and utilized for sensitive backup data storage.	No exceptions noted.
	Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.	Inspected the policies and procedures to determine that new user access, modification, and removal policies are in place.	No exceptions noted.	

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	<p>system credentials are removed when user access is no longer authorized.</p>	<p>Human Resources management utilizes an onboarding checklist to ensure that specific elements of the hiring process are consistently executed. A copy of the onboarding checklist is maintained in the employee file.</p> <p>Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.</p> <p>Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. This includes but is not limited to the terminated employee's physical and logical access to company facilities and computer systems. The checklist is retained in the employee files.</p> <p>A periodic review of network access lists is performed by administrators to ensure that only appropriate individuals have active accounts in the domain.</p>	<p>Inspected a judgmental sample of ConnectWise onboarding tickets used for employees hired during the review period to determine that HR management utilizes an onboarding checklist for the employees and that the checklist is retained in the employee files.</p> <p>Inspected the default domain user listing and a judgmental sample of production server user listings to determine that management revoked network access privileges assigned to terminated employees as a component of the employee termination process.</p> <p>Inspected a judgmental sample of ConnectWise tickets utilized during the review period, to determine that Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process including access removal are consistently executed, and that the checklists are retained in the employee files.</p> <p>Inquired of management to determine that a periodic review of network access lists is performed by administrators to ensure that</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3	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.	<p>Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.</p> <p>Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.</p> <p>Management has segregated specific duties within the production environment for administering critical areas such as:</p> <ul style="list-style-type: none"> • Network administration • Systems (including Active Directory) administration. <p>Management has segregated specific duties within the internal network domain for administering critical areas such as network administration and database management. Management restricts network domain administration privileges to approved positions only.</p>	<p>only appropriate individuals have active accounts in the domain.</p> <p>Inspected the policies and procedures to determine that new user access, modification, and removal policies are in place.</p> <p>Inspected the default domain user listing and a judgmental sample of production server user listings to determine that management revoked network access privileges assigned to terminated employees as a component of the employee termination process.</p> <p>Inspected access rights listing to determine that management has segregated specific duties within the production environment for administering critical areas.</p> <p>Inquired of management to determine that management has authorized specific personnel to administer information security within the internal network domain, and has segregated duties.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the production environment, and has segregated specific duties within the internal network domain for administering critical areas such as network administration, and database management.	No exceptions noted.
		A periodic review of network access lists is performed by administrators to ensure that only appropriate individuals have active accounts in the domain.	Inquired of management to determine that a periodic review of network access lists is performed by administrators to ensure that only appropriate individuals have active accounts in the domain.	No exceptions noted.
		designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers have physical access controls in place to <i>restrict access</i> to authorized personnel only.	Inspected the most recent SOC audit reports for the various third party data centers to determine that the various third party data centers have physical access controls in place to <i>restrict access</i> to authorized personnel only.	No exceptions noted.
		designDATA management reviews the SOC audit reports of the various third party data centers annually and documents the results of the reviews of the SOC audit reports in a memo.	Inquired of management to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.	No exceptions noted.
			Inspected management's memo to determine that designDATA management documents the	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4	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.	Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.	results of the reviews of the SOC reports in a memo. Inspected the policies and procedures manual to determine that physical security policies and procedures were in place to guide personnel regarding restricting access to the facility.	No exceptions noted.
		designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers have physical access controls in place to <i>restrict access</i> to authorized personnel only.	Inspected the most recent SOC audit reports for the various third party data centers to determine that the various third party data centers have physical access controls in place to <i>restrict access</i> to authorized personnel only.	No exceptions noted.
		designDATA management reviews the SOC audit reports of the various third party data centers annually and documents the results of the reviews of the SOC audit reports in a memo.	Inquired of management to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.	No exceptions noted.
			Inspected management's memo to determine that designDATA management documents the results of the reviews of the SOC reports in a memo.	No exceptions noted.
CC6.5	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	Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.	Inspected the policies and procedures manual to determine that physical security policies and procedures were in place to guide personnel regarding restricting access to the facility.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	and is no longer required to meet the entity's objectives.	<p>Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.</p> <p>designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers have physical access controls in place to <i>remove access</i> when no longer required.</p> <p>designDATA management reviews the SOC audit reports of the various third party data centers annually and documents the results of the reviews of the SOC audit reports in a memo.</p>	<p>Inspected the default domain user listing and a judgmental sample of production server user listings to determine that management revoked network access privileges assigned to terminated employees as a component of the employee termination process.</p> <p>Inspected the most recent SOC audit reports for the various third party data centers to determine that the various third party data centers have physical access controls in place to <i>remove access</i> when no longer required.</p> <p>Inquired of management to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.</p> <p>Inspected management's memo to determine that designDATA management documents the results of the reviews of the SOC reports in a memo.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Procedures have been implemented to provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.</p>	<p>procedures to guide personnel regarding sharing information with third parties.</p> <p>Inspected confidentiality policies and procedures related to disclosure to third parties to determine that confidential information is disclosed to third parties is done in accordance with the entity's defined confidentiality and related security policies.</p>	No exceptions noted.
		<p>Firewall systems are in place to screen data flow between external parties and the designDATA network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.</p>	<p>Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and designDATA network.</p>	No exceptions noted.
		<p>The firewall requires two factor authentication before administrative access to the firewall system is allowed.</p>	<p>Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.</p>	No exceptions noted.
		<p>All firewall administrator accounts have been changed from their default passwords.</p>	<p>Observed the network engineer log into the firewall system to determine that the firewall required two factor authentication before administrative access to the firewall system was allowed.</p> <p>Inspected the administrator account password configurations to determine that all firewall</p>	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The ability to modify the firewall system software, configurations or rule sets is restricted based on job responsibility and is limited to approved positions only.	administrator accounts have been changed from their default passwords. Inspected firewall system access documentation to determine that the ability to modify the firewall system software, configuration or rule sets is restricted based on job responsibility and is limited to approved positions only.	No exceptions noted.
		Administrative access to the firewall system is restricted to allowed network segments.	Inspected the access rules to determine that the ability to access the firewall system remotely is restricted.	No exceptions noted.
		Firewalls are configured to log all access and modifications to the firewall system software, and logs are available for ad hoc review by security personnel.	Inquired of management to determine that all modifications to the firewall system software, configurations or rule sets are logged and available for ad hoc review by security personnel.	No exceptions noted.
		Firewalls are configured to log all blocked packets which might indicate potentially malicious activity, and logs are available for ad hoc review by security personnel.	Inspected a judgmental sample of logs of modifications to the firewall system software, configurations or rule sets to determine that they are logged. Inspected the firewall system configuration and sample firewall system logs to determine that firewalls are configured to log all blocked packets.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Hardware and software-based firewalls and routers are placed at all network perimeter and third-party entry points to designDATA networks.</p> <p>Multiple production firewalls are utilized for redundancy. The firewalls are set up in an active/passive configuration with automatic failover in the event of failure of the primary.</p> <p>Firewall configurations filter internet traffic based on content and destination site address. The configurations include:</p> <ul style="list-style-type: none"> • The firewall performs stateful packet inspection. • Network Address Translation (NAT) services are enabled on all network firewalls to hide internal servers. • Firewall ports are configured to allow only specific types of traffic between 	<p>Inspected the network diagram, router security policy, and firewall system rule sets to determine that hardware and software-based firewalls and routers are placed at all network perimeter and third party entry points to designDATA networks.</p> <p>Observed the network firewalls and routers to determine that hardware and software-based firewalls and routers are placed at all network perimeter and third-party entry points to designDATA networks.</p> <p>Inspected the network diagram to determine that multiple firewalls are setup for redundancy.</p> <p>Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.</p> <p>Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address, and that the firewall performs stateful packet inspection.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>certain destinations. All unused ports on the firewall are blocked.</p> <ul style="list-style-type: none"> • The firewall is configured to deny all traffic that is not specifically authorized in the rule set. <p>designDATA actively utilizes the following firewall features for protection at the perimeter of the network and between network segments:</p> <ul style="list-style-type: none"> • Stateful packet inspection • IPsec / Remote Ethernet Device (RED) site-to-site tunnel • TLS client-based VPN • Intrusion Detection and Prevention • Advance Threat Protection • Logging and • Reporting. 	<p>Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.</p> <p>Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.</p> <p>Inspected the firewall documentation to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.</p> <p>Inspected firewall configurations to determine that designDATA actively utilizes the stated firewall features for protection at the perimeter of the network and between network segments.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The production network is logically and physically segregated from the internal corporate network.	Inspected a network diagram to determine that the production network was logically and physically segregated from the internal corporate network.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC6.7	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.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures to guide personnel regarding sharing information with third parties.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security breaches and other incidents.	No exceptions noted.
		Only authorized system administrators are able to install software on system devices.	Inquired of management to determine that only authorized system administrators are able to install software on system devices.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Third party antivirus software is installed on all designDATA servers (endpoint protection).</p> <p>designDATA maintains current virus signature updates. Antivirus definitions are monitored for updates by a central antivirus server every four hours. Individual machines have application agents that are installed and configured through a central monitoring console. Updates are pulled to specific production servers hourly.</p> <p>For server patching, an automated methodology is utilized to monitor patch releases. Updates are managed through a central application (Kaseya), which automatically pushes patch updates to servers if appropriate.</p>	<p>Inquired of management to determine that third party antivirus software is installed on all designDATA servers.</p> <p>Inspected antivirus software installed on judgmental sample of designDATA servers to determine that antivirus software is installed on all designDATA servers.</p> <p>Inspected the antivirus software documentation to determine that a central server monitored for updates to antivirus definitions hourly.</p> <p>Inspected the list of servers configured to pull updates from the central antivirus server to determine that antivirus software was installed on specific production servers.</p> <p>Inspected the antivirus software documentation to determine that updates were pulled to specific production servers hourly.</p> <p>Inquired of management to determine that a methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>designDATA IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.</p>	<p>Inspected the monitoring application to determine that a scan schedule is utilized to monitor patch releases, and distribute patches to relevant devices.</p> <p>Inspected a sample of informational service communications to determine that IT personnel utilize security issue monitoring services.</p> <p>Inquired of management to determine that designDATA IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1	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.	<p>Third party enterprise monitoring applications are used to monitor and record performance criteria for critical <i>designDATA</i> server and network equipment.</p> <p>A third party enterprise monitoring application is used to monitor and record performance criteria for contracted <i>client</i> server and network equipment.</p> <p>System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.</p> <p>The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via text or email to appropriate support personnel.</p>	<p>Inspected the Kaseya enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical <i>designDATA</i> server and network equipment.</p> <p>Inspected the enterprise monitoring application to determine that a third party enterprise monitoring application is used to monitor performance criteria for contracted <i>client</i> server and network equipment.</p> <p>Inspected the Kaseya metrics tracking reports to determine that system downtime and operations issues were monitored.</p> <p>Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
CC7.2	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	For server patching, an automated methodology is utilized to monitor patch releases. Updates are managed through a central application (Kaseya), which automatically pushes patch updates to servers if appropriate.	Inquired of management to determine that a methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	analyzed to determine whether they represent security events.	<p>designDATA IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.</p> <p>Management periodically performs internal security assessments, including reviews of server logs and other critical items.</p> <p>Monthly full backups are performed of critical company data such as critical application and database components. Logs are used to record backup activity.</p>	<p>Inspected the monitoring application to determine that a scan schedule is utilized to monitor patch releases, and distribute patches to relevant devices.</p> <p>Inspected a sample of informational service communications to determine that IT personnel utilize security issue monitoring services.</p> <p>Inquired of management to determine that designDATA IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.</p> <p>Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.</p> <p>Inspected a judgmental sample of backup software logs to determine that monthly full data backups are performed of all critical designDATA data such as critical application and database components.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Backup jobs are monitored for failure by authorized personnel.</p> <p>Failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email. Failures are investigated and resolved.</p> <p>The backup applications generate and maintain logs, which specify the data backup processes are completed, and success/failure status of each process.</p> <p>Management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.</p>	<p>Observed backup monitoring process to determine that backup jobs are monitored for failure by authorized personnel.</p> <p>Inquired of management to determine that failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.</p> <p>Inspected a judgmental sample of emailed notifications to determine that failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.</p> <p>Inspected the backup application logs to determine that backup applications maintain logs which specify the data backup processes are completed, and success/failure status of each process.</p> <p>Inquired of management to determine that management performs systematic reviews of the backup application and logs to detect abnormalities in the backup process.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3	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.		Inspected a judgmental sample of backup application logs or reports to determine that management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.	No exceptions noted.
		Firewalls are configured to log all access and modifications to the firewall system software, and logs are available for ad hoc review by security personnel.	Inquired of management to determine that all modifications to the firewall system software, configurations or rule sets are logged and available for ad hoc review by security personnel.	No exceptions noted.
			Inspected a judgmental sample of logs of modifications to the firewall system software, configurations or rule sets to determine that they are logged.	No exceptions noted.
		Firewalls are configured to log all blocked packets which might indicate potentially malicious activity, and logs are available for ad hoc review by security personnel.	Inspected the firewall system configuration and sample firewall system logs to determine that firewalls are configured to log all blocked packets.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
Policies and procedures are in place to guide personnel regarding addressing how complaints	Inspected the policies and procedures to determine that the	No exceptions noted.		

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>and requests relating to security issues are resolved.</p> <p>An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.</p> <p>A ticketing system is utilized to manage systems infrastructure issues and changes. Tickets are assigned to support personnel based on the nature of the ticket.</p> <p>Helpdesk calls are entered into the ticketing system and call tracking utility and given a ticket number.</p> <ul style="list-style-type: none"> • A priority level is assigned in accordance with company policy. • All issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution. • Call volume and open tickets are reviewed in regularly scheduled helpdesk staff meetings. • All closed tickets are communicated to the Requestor, either automatically via email from the tracking utility, or manually by IT helpdesk staff. 	<p>entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.</p> <p>Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.</p> <p>Inspected a judgmental sample of logs from the ConnectWise ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.</p> <p>Inquired of management to determine that helpdesk calls are entered into the call tracking utility and given a ticket number, a priority level is assigned in accordance with company policy, and all issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected a judgmental sample of reports generated for staff meetings and closed ticket emails to determine that call volume and open tickets are reviewed in regularly scheduled helpdesk staff meetings, and that all closed tickets are communicated to the requestor, either automatically via email from the tracking utility, or manually by IT helpdesk staff.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	<p>Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.</p> <p>Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.</p> <p>An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.</p>	<p>Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.</p> <p>Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.</p> <p>Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.</p> <p>An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.</p> <p>A ticketing system is utilized to manage systems infrastructure issues and changes. Tickets are assigned to support personnel based on the nature of the ticket.</p> <p>Helpdesk calls are entered into the ticketing system and call tracking utility and given a ticket number.</p> <ul style="list-style-type: none"> • A priority level is assigned in accordance with company policy. • All issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution. 	<p>procedures regarding identifying and mitigating system security and related security breaches and other incidents.</p> <p>Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.</p> <p>Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.</p> <p>Inspected a judgmental sample of logs from the ConnectWise ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.</p> <p>Inquired of management to determine that helpdesk calls are entered into the call tracking utility and given a ticket number, a priority level is assigned in accordance with company policy, and all issues that cannot be addressed within appropriate time intervals are escalated to</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<ul style="list-style-type: none"> • Call volume and open tickets are reviewed in regularly scheduled helpdesk staff meetings. • All closed tickets are communicated to the Requestor, either automatically via email from the tracking utility, or manually by IT helpdesk staff. 	<p>management to assure timely resolution.</p> <p>Inspected a judgmental sample of reports generated for staff meetings and closed ticket emails to determine that call volume and open tickets are reviewed in regularly scheduled helpdesk staff meetings, and that all closed tickets are communicated to the requestor, either automatically via email from the tracking utility, or manually by IT helpdesk staff.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	Inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	No exceptions noted.
		Policies and procedures are in place for classifying data based on its criticality and sensitivity and that classification is one of many factors used to define protection requirements, access rights and restrictions, and retention and destruction requirements.	Inspected the policies and procedures to determine that data classification, protection requirements, access rights, access restrictions, and retention and destruction policies were established.	No exceptions noted.
		Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding assigning responsibility and accountability for system changes and maintenance.	No exceptions noted.
		Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Observed and inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Policies and procedures are in place to guide personnel regarding testing, evaluating, and authorizing system components before implementation.</p> <p>A ticketing system is utilized to manage systems infrastructure issues and changes. Tickets are assigned to support personnel based on the nature of the ticket.</p> <p>Routine network maintenance is scheduled by the data centers at early morning weekend hours, and email ticketing notification is automatically generated to designDATA IT personnel.</p> <p>A standard hardware build is utilized for installation and maintenance of certain critical designDATA servers.</p>	<p>operating effectiveness of controls are identified during system operation and monitoring.</p> <p>Inspected the policies and procedures related to testing, evaluating, and authorizing before implementation of components.</p> <p>Inspected a judgmental sample of logs from the ConnectWise ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.</p> <p>Inspected a judgmental sample of notifications from the data centers to determine that routine network maintenance is scheduled by the data centers at early morning weekend hours, and email ticketing notification is automatically generated to designDATA's IT personnel.</p> <p>Inspected the standard hardware build procedures for certain designDATA servers to determine that a standard hardware build is utilized for certain critical designDATA servers.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Network administrators harden servers by enabling only necessary operating system services and roles, and factory default configurations are changed as appropriate:</p> <ul style="list-style-type: none"> • Non-essential default accounts are turned off • Non-essential services are turned off • FTP access is disabled for non-FTP servers • Security event logging is enabled. <p>A standard vHost template for virtualized environments is utilized for installation and maintenance of certain critical designDATA and customer virtual machines.</p> <p>Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.</p> <p>For server patching, an automated methodology is utilized to monitor patch releases. Updates are managed through a central application (Kaseya), which automatically pushes patch updates to servers if appropriate.</p>	<p>Inquired of management to determine that network administrators harden servers by enabling only necessary operating system services and roles.</p> <p>Inspected the vHost configurations to determine that a standard template is used for installation and maintenance of certain critical designDATA virtual machines.</p> <p>Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.</p> <p>Inspected current agreements with third party vendors to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.</p> <p>Inquired of management to determine that a methodology is utilized to monitor patch releases, distribute patches to relevant</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Infrastructure changes and patches to third party applications are tested by the technical support department being applied to production servers.</p> <p>Management has a data classification methodology to identify and classify sensitive data in the production environment.</p> <p>designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers are responsible for the general IT controls relevant to their application development.</p>	<p>devices and apply the patches to the device.</p> <p>Inspected the monitoring application to determine that a scan schedule is utilized to monitor patch releases, and distribute patches to relevant devices.</p> <p>Inquired of management to determine that infrastructure changes tested by the technical support department after hours before being introduced to production servers.</p> <p>Inspected hardware update logs to determine that patches and upgrades to critical services are tested by the technical support department being introduced to a production server.</p> <p>Inquired of management to determine that management has a data classification methodology to identify and classify sensitive data.</p> <p>Inspected the most recent SOC audit reports for the various third party data centers to determine that the various third party data centers are responsible for the general IT controls relevant to their application development.</p>	<p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers are responsible for the general IT controls relevant to their change management.</p> <p>designDATA management reviews the SOC audit reports of the various third party data centers annually and documents the results of the reviews of the SOC audit reports in a memo.</p>	<p>Inspected the most recent SOC audit reports for the various third party data centers to determine that the various third party data centers are responsible for the general IT controls relevant to their change management.</p> <p>Inquired of management to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.</p> <p>Inspected management's memo to determine that designDATA management documents the results of the reviews of the SOC reports in a memo.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC9.0 - COMMON CRITERIA RELATED TO RISK MITIGATION

The criteria relevant to how the entity identifies, selects and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	<p>A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas:</p> <ul style="list-style-type: none"> • Data security (company data and client data) • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information • Regulatory, economic, and physical environment in which the company operates • Business environment, including industry, competitors, regulatory environment, and consumers • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies • Management and respective attitudes and philosophies on the system of internal control • Vendor and business partner relationships including third party data centers • Systems and technology environment. 	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC9.0 - COMMON CRITERIA RELATED TO RISK MITIGATION

The criteria relevant to how the entity identifies, selects and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	<p>Procedures have been implemented to provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.</p> <p>Procedures have been implemented to obtain assurance or representation that the policies of third parties to whom information is transferred are in conformity with the designDATA policies related to confidentiality.</p> <p>Prior to collecting personal information of external users, a privacy policy is provided that may include the purpose and use of the personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, and disposal of personal information.</p> <p>A non-disclosure or confidentiality agreement is in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity.</p>	<p>Inspected confidentiality policies and procedures related to disclosure to third parties to determine that confidential information is disclosed to third parties is done in accordance with the entity's defined confidentiality and related security policies.</p> <p>Inspected confidentiality policies and procedures implemented which help to obtain assurance or representation that the policies of third parties to whom information is transferred are in conformity with the designDATA policies related to confidentiality.</p> <p>Inspected policies to determine that if personal information of external users is collected, a privacy policy is provided that may include the purpose and use of the collection of their personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, and disposal of personal information.</p> <p>Inspected a judgmental sample of agreements to determine that a non-disclosure or confidentiality agreement is in place with related</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC9.0 - COMMON CRITERIA RELATED TO RISK MITIGATION

The criteria relevant to how the entity identifies, selects and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			parties and vendors and that they include confidentiality commitments applicable to that entity.	

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Principle and Criteria Table

The availability category refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	<p>Policies and procedures are in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.</p> <p>Policies and procedures are in place for identifying and documenting the system availability and related security requirements of authorized users.</p>	<p>Inspected the policies and procedures to determine that policies and procedures were in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.</p> <p>Inspected the policies and procedures to determine that the entity’s system availability and related security policies were established.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	<p>Policies and procedures are in place to guide personnel regarding the identification of and consistency with defined commitments, service-level agreements, and other contractual requirements.</p> <p>designDATA utilizes various third party data centers for housing certain critical production computer servers, applications, and networking equipment. The environmental security and maintenance controls at the various third party data centers are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.</p>	<p>Inspected the policies and procedures and the service level agreements to determine that the entity’s policies included procedures regarding the identification of and consistency with defined commitments, service-level agreements, and other contractual requirements.</p> <p>Inspected the most recent SOC audit reports for the various third party data centers to determine that the environmental security and maintenance controls at the various third party data centers are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Principle and Criteria Table

The availability category refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The various third party data centers are responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by designDATA.</p> <p>designDATA management reviews the SOC audit reports of the various third party data centers annually and documents the results of the reviews of the SOC audit reports in a memo.</p> <p>A third party automated backup application (Veeam) is utilized to perform scheduled system image-based disk-to disk backups. This results in multiple copies of production data, including:</p> <ol style="list-style-type: none"> 1. Production data 2. Backup copy on Exagrid appliance 3. Replicated copy at redundant data center 4. Monthly copy to tape (see below). <p>The backups are asynchronous.</p> <ul style="list-style-type: none"> • Point-in-time snapshots (recovery points) are made once per day. • These incremental backups are combined once a week to create a continuous “synthetic full” image. 	<p>Inspected the most recent SOC audit reports for the various third party data centers to determine that designDATA utilizes relevant reports provided by the various third party data centers.</p> <p>Inquired of management to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.</p> <p>Inspected management’s memo to determine that designDATA management documents the results of the reviews of the SOC reports in a memo.</p> <p>Inspected the third party automated backup system to determine that automated backup systems are utilized to perform scheduled system backups.</p> <p>Inspected the backup storage control panel to determine that backups are made to a backup server, and that recovery points have been configured as needed.</p>	<p>No exceptions noted.</p>

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Principle and Criteria Table

The availability category refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>The retention period for backup data is 21 restore points.</p> <p>Systems that are backed up include:</p> <ul style="list-style-type: none"> • SQL servers • Exchange servers • Active directory servers • Application servers. <p>Veeam is utilized to create tape backups of Veeam disk-to-disc backup jobs. The backup jobs are created and scheduled by authorized personnel.</p> <p>Monthly full backups are performed of critical company data such as critical application and database components. Logs are used to record backup activity.</p> <p>Multiple external backup tapes are used in rotation as backup media for backup procedures. While at the data center, they are automated by a 48-slot tape robot.</p> <p>Backup tapes are moved from the third party data center to the main office once per month. Backup tapes are maintained in a locked filing cabinet in a secure storage room at all times while on company premises.</p> <p>Backup media are rotated off-site according to a formal rotation schedule.</p>	<p>Inspected a judgmental sample of backup data jobs to determine that the retention period is 21 restore points.</p> <p>Inspected list of servers configured to be backed up to disk to determine that the enumerated servers are backed up.</p> <p>Inspected judgmental sample of backup scheduling to determine that backup jobs are created and scheduled by authorized personnel.</p> <p>Inspected a judgmental sample of backup software logs to determine that monthly full data backups are performed of all critical designDATA data such as critical application and database components.</p> <p>Inquired of management to determine that multiple backup tapes are used in rotation as backup media.</p> <p>Observed locked cabinet in secure storage room to determine that backup tapes are maintained in a secure location at all times while on company premises.</p> <p>Inspected the rotation schedule for backup media to determine that</p>	<p>No exceptions noted.</p>

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Principle and Criteria Table

The availability category refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Backup jobs are monitored for failure by authorized personnel.</p> <p>Failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email. Failures are investigated and resolved.</p> <p>The backup applications generate and maintain logs, which specify the data backup processes are completed, and success/failure status of each process.</p> <p>Management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.</p>	<p>backup media are rotated off-site according to a formal rotation schedule.</p> <p>Observed backup monitoring process to determine that backup jobs are monitored for failure by authorized personnel.</p> <p>Inquired of management to determine that failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.</p> <p>Inspected a judgmental sample of emailed notifications to determine that failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.</p> <p>Inspected the backup application logs to determine that backup applications maintain logs which specify the data backup processes are completed, and success/failure status of each process.</p> <p>Inquired of management to determine that management performs systematic reviews of the backup application and logs to detect abnormalities in the backup process.</p>	<p>No exceptions noted.</p>

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Principle and Criteria Table

The availability category refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected a judgmental sample of backup application logs or reports to determine that management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.	No exceptions noted.
		Policies and procedures are in place to govern critical computer operations activities.	Inspected the policies and procedures to determine that policies and procedures are in place to govern critical computer operations activities.	No exceptions noted.
		An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner and to properly document them.	Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.	No exceptions noted.
		Redundant internet connections are in place through multiple telecommunications providers, with separate optical fiber entrances into the physical building, and multiple routers and switches are utilized. Failover is controlled by BGP at the router level.	Inspected network diagram to determine that redundant internet connections are in place, through multiple providers with separate optical fiber entrances into the physical building, and that multiple routers and switches are utilized.	No exceptions noted.
			Inspected failover configurations to determine that the firewall controls failover and that it is configured in an active-passive configuration.	No exceptions noted.
		Multiple lines of communication to telecommunications providers are configured in an active-active configuration, and multiple routers and switches provide automatic redundancy in the event of communications	Inspected the internet connection failover alert configurations in the router interface to determine that multiple internet connections provide active-active redundancy,	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Principle and Criteria Table

The availability category refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	<p>disruption. In the event of failure of one or more lines, the enterprise monitoring system sends alert notifications.</p> <p>designDATA utilizes fully redundant routing and switching equipment for its core networking infrastructure.</p> <p>Policies and procedures are in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.</p> <p>Management periodically performs restorations of backup data at customer request, which serves to verify the success of backup processes and employee readiness.</p>	<p>and that in the event of failure of one or more lines, the enterprise monitoring system sends alert notifications.</p> <p>Inspected network diagram to determine that designDATA utilizes fully redundant routing and switching equipment for its core networking infrastructure.</p> <p>Inspected the policies and procedures and service level agreements to determine that policies and procedures were in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.</p> <p>Inquired of management to determine that management periodically performs restorations of backup data at customers’ request, which serves to verify the success of backup processes and employee readiness.</p> <p>Inspected a judgmental sample of restoration logs to determine that management periodically performs restorations of backup data at customer request, which serves to verify the success of backup processes and employee readiness.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 3 ADDITIONAL CRITERIA FOR CATEGORY OF CONFIDENTIALITY

Confidentiality Category and Criteria Table

The confidentiality category refers to the entity’s ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity’s control in accordance with management’s objectives.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.	<p>Policies and procedures are in place to communicate retention periods for confidential information maintained by designDATA. Procedures are in place to:</p> <ul style="list-style-type: none"> • Automatically delete confidential information in accordance with specific retention requirements; • Delete backup information in accordance with defined schedules; • Require approval for confidential information to be retained beyond its retention period; and • Review annually information marked for retention. 	<p>Inspected designDATA’s retention policies for confidential information to determine that the policies included procedures to:</p> <ul style="list-style-type: none"> • Automatically delete confidential information in accordance with specific retention requirements; • Delete backup information in accordance with defined schedules; • Require approval for confidential information to be retained beyond its retention period; and • Review annually information marked for retention. 	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	<p>Policies and procedures are in place to communicate designDATA’s destruction policy for confidential information.</p> <p>The entity:</p> <ul style="list-style-type: none"> • locates and removes or redacts specified confidential information as required; • regularly and systematically destroys, erases, or makes anonymous confidential information that is no longer required for the purposes identified in its confidentiality commitments or system requirements; 	<p>Inspected the destruction policy to determine that policies and procedures are in place to communicate designDATA’s destruction policy for confidential information.</p> <p>Inquired of management to determine that the entity:</p> <ul style="list-style-type: none"> • locates and removes or redacts specified confidential information as required; • regularly and systematically destroys, erases, or makes anonymous confidential 	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

MATRIX 3 ADDITIONAL CRITERIA FOR CATEGORY OF CONFIDENTIALITY

Confidentiality Category and Criteria Table

The confidentiality category refers to the entity’s ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity’s control in accordance with management’s objectives.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<ul style="list-style-type: none"> • erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based); • disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies; and • documents the disposal of confidential information. 	<p>information that is no longer required for the purposes identified in its confidentiality commitments or system requirements;</p> <ul style="list-style-type: none"> • erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based); • disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies; and • documents the disposal of confidential information. <p>Inspected documentation to determine that the entity documents the disposal of confidential information.</p>	<p>No exceptions noted.</p>

END OF REPORT