designDATA

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 Principles of Security, Availability, and Confidentiality

For the Period June 1, 2017 to May 31, 2018

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

The Moore Group, CPA
SOC Audit Specialists

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 the description in Section 3 titled "Description of the Service Organization's System Provided by designDATA Management" (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability, and confidentiality principles set forth in TSP Section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria), throughout the period June 1, 2017 to May 31, 2018.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of designDATA's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

As indicated in the description, designDATA uses various service organizations (subservice organizations) to perform aspects of its data center and managed services and systems. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed and operating effectively. The description presents designDATA's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period June 1, 2017 to May 31, 2018.

Service Organization's Responsibilities

In Section 2, designDATA has provided its assertion titled "Assertions by the Service Organization's Management" (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. designDATA is 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; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period June 1, 2017 to May 31, 2018.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves—

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period June 1, 2017 to May 31, 2018.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in designDATA's assertion and the applicable trust services criteria—

a. the description fairly presents the system that was designed and implemented throughout the period June 1, 2017 to May 31, 2018.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period June 1, 2017 to May 31, 2018, and the subservice organization applied the types of controls expected to be implemented at the subservice organizations throughout the period June 1, 2017 to May 31, 2018, and user entities applied the complementary user entity controls contemplated in the design of designDATA’s controls throughout the period June 1, 2017 to May 31, 2018.

c. the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period June 1, 2017 to May 31, 2018 if the controls expected to be implemented at the subservice organizations were also operating effectively throughout the period June 1, 2017 to May 31, 2018 and if user entities applied the complementary user entity controls contemplated in the design of designDATA's controls, and those controls operated effectively throughout the period June 1, 2017 to May 31, 2018.

Description of Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are listed in Section 4, titled "Testing Matrices" of this report.

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, 2017 to May 31, 2018; and prospective user entities, independent auditors, and practitioners providing services to such user entities, 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, subservice organizations, and other parties.
- Internal control and its limitations.
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

The Moore Group CPA, LLC

Nashua, NH
July 2, 2018

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 attached description of DesignDATA's (designDATA) data center and managed services and systems (the description) based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) (description criteria). The description is intended to provide users with information about the data center and managed services and system controls particularly intended to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services principles) throughout the period June 1, 2017 to May 31, 2018. We confirm, to the best of our knowledge and belief, that

1) The description fairly presents the data center and managed services and systems throughout the period June 1, 2017 to May 31, 2018. designDATA uses various third party data centers to perform aspects of its data center and managed services and systems. The description includes only the applicable trust services criteria and related controls of designDATA and excludes the applicable trust services criteria and related controls of the third party data centers. Our assertion is based on the following description criteria:

    a) The description contains the following information:

        i) The types of services provided.

        ii) The components of the system used to provide the services, which are as follows:

            (1) Infrastructure. The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

            (2) Software. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

            (3) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

            (4) Processes. The automated and manual procedures.

            (5) Data. Transaction streams, files, databases, tables, and output used or processed by a system.

        iii) The boundaries or aspects of the system covered by the description.

        iv) For information provided to, or received from, subservice organizations, and other parties—

            (1) how the information is provided or received and the role of the subservice organizations and other parties.

            (2) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

        v) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(1) Complementary user entity controls contemplated in the design of the service organization’s system.

(2) When the inclusive method is used to present a subservice organization, controls at the subservice organization.

vi) If the service organization presents the subservice organization using the carve-out method—

(1) the nature of the services provided by the subservice organization.

(2) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

vii) Any applicable trust services criteria that are not addressed by a control and the reasons.

viii) In the case of a Type 2 report, relevant details of changes to the service organization’s system during the period covered by the description.

b) The description does not omit or distort information relevant to the service organization’s system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

2) The controls stated in the description were suitably designed throughout the period June 1, 2017 to May 31, 2018 to meet the applicable trust services criteria.

3) The controls stated in the description operated effectively throughout the period June 1, 2017 to May 31, 2018 to meet the applicable trust services criteria.

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.

<u>System Boundaries</u>
As outlined in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy, 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:

<u>Data Center Services</u>
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 24×7 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 24×7
- 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

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 a SOC 1 Type II report for the period July 1, 2016 to June 30, 2017. 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 plus HiTrust report for the period January 1, 2017 to December 31, 2017. 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 services provided to user organizations. The applications run on Windows Server platforms with SQL databases to support the applications.

People

designDATA is led by its President and CEO, Dennis 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:

- 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.
- 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/SSL VPN
  - Intrusion Detection and Prevention
  - Advance Threat Protection
  - Logging and
  - Reporting.
- Users are required to authenticate via a unique user ID and password before being granted access to designDATA internal network domain.
- 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.

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/SSL VPN
  - Intrusion Detection and Prevention
  - Advance Threat Protection
  - Logging and
  - Reporting.

Disaster Recovery

designDATA maintains a current Disaster Recovery Plan and Business Continuity plan. Disaster and business continuity emergency situations are ultimately managed through proper planning (crisis management, recovery and continuity) and response. Identified risks have been mitigated through prevention, minimization or rapid recovery resources and planning. designDATA's disaster recovery and business continuity program helps to ensure that disruptive incidents are responded to quickly and effectively.

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.
- Periodic **meetings with staff** are conducted whereby the core values and mission of designDATA are discussed as well as ways to reinforce and improve the components of designDATA's related core functions.
- Comprehensive **background checks** are performed by an independent third party for all employees as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for positions within designDATA.
- 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.
- 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.

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 is guided by designDATA's corporate **mission statement** in determining the implementation of corporate goals and operational activities to meet them.
- 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 any regulatory compliance or operational trends affecting the services provided.
- **Management meetings** are held on a regular basis to discuss operational planning and budgeting, human resource planning and hiring, and customer related issues. Meeting agendas and meeting minutes are recorded and communicated to relevant personnel.

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.
- designDATA's **operating goals and objectives are communicated** to the entire organization during regular staff meetings, employee performance reviews, and other written communications.
- designDATA provides an **employee orientation program** that communicates organizational structure and responsibility, company and departmental objectives, and relationships between departments and personnel.
- designDATA has established a **segregation of duties process**, which is based upon changes and recommendations from management.

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.

- Management has established **hiring guidelines and procedures** that guide the hiring process to ensure that specific elements of the hiring process are consistently executed. This includes the use of an independent, outsourced HR services provider.
- Human Resources management utilizes a **new hire checklist** to ensure that specific elements of the hiring process are consistently executed. A copy of the new hire checklist is maintained in the employee file.

- Each new employee undergoes a monthly one-on-one **performance review** to evaluate performance.
- Each employee undergoes an **annual performance review** each year. During these reviews, management reinforces and updates professional development plans for each employee. A formal evaluation form is prepared, and is maintained in employee's HR file.
- Management has established **employee termination procedures** that guide the termination process.
- 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

- 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 platforms with SQL 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.

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.
- User organizations are responsible for developing their own disaster recovery and business continuity plans that address their ability to access or utilize designDATA services.
- 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.
- 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.
- 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.
- User organizations are responsible for requesting the revocation of application access privileges assigned to terminated employees as a component of the employee termination process.
- 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.
- User organizations are responsible for notifying designDATA of changes made to technical or administrative contact information in a timely manner.
- User organizations are responsible for understanding and defining data storage requirements.
- User organizations are responsible for understanding and implementing encryption protocols to protect data during transfer to designDATA.
- User organizations are responsible for immediately notifying designDATA of any actual or suspected information security breaches, including compromised user accounts and passwords.
- User organizations are responsible for notifying designDATA of any regulatory issues that may affect the services provided by designDATA.

SECTION 4

TESTING MATRICES

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	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.
		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.	Inquired of management regarding communication of organizational charts to determine that the charts are communicated to employees and updated as needed.	No exceptions noted.
			Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority and responsibility and are updated as needed.	No exceptions noted.
		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.	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	No exceptions noted.

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			close oversight maintained by the CEO.	
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	A policy is in place to assign responsibility and accountability for developing and maintaining the entity’s security, availability, and confidentiality policies, and changes and updates to those policies, to appropriate personnel.	Inspected the policies and procedures to determine that responsibility and accountability for developing and maintaining the entity’s system security, availability, and confidentiality policies, and changes and updates to those policies, were assigned to appropriate personnel.	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.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting	Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security, availability, and confidentiality 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, availability, and confidentiality policies.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	security, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.			
		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 utilizes skills assessment testing for certain positions during the hiring process.	No exceptions noted.
		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.	Inquired of management into initial and ongoing training and development for employees, to determine that a program is in place.	No exceptions noted.
			Inspected a judgmental sample of company documentation (meeting agendas, assignments) of initial training and development for new employees.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			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.	No exceptions noted.
		Management encourages employees to complete and continue formal education and technical certification programs.	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.	No exceptions noted.
			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.
		Management-approved professional development expenses incurred by the employees are paid by designDATA.	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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	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.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.
		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.	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.	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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	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.
		Network diagrams are in place and communicated to appropriate personnel.	Inspected network diagrams to determine that network diagrams are in place and communicated to appropriate personnel.	No exceptions noted.
CC2.2	The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Policies and procedures are in place for identifying and documenting the system security, availability, and confidentiality requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system security, availability, and confidentiality 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.
		New client contracts are approved by designDATA management prior to initiating service. A Service Level Agreement (SLA) is	Inspected a judgmental sample of new client contracts and SLAs formalized during the review period	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		signed by the client and designDATA management.	to determine that they are signed off by the client and designDATA management.	
		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.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.
		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.	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.	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.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policies and procedures are in place to assign responsibility and accountability for system security, availability, and confidentiality.	Inspected the policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system security, availability, and confidentiality.	No exceptions noted.
		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.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.
		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.	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.	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	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			client information, to unauthorized parties.	
		Documented backup procedures are in place for *customer* system backups performed by designDATA.	Inspected documented backup procedures to determine that documented backup procedures are in place for critical customer systems.	No exceptions noted.
		Data backups of contracted *customer* application components and databases are performed according to the timing reflected in the customer contract.	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.	No exceptions noted.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.	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 guide personnel regarding the identification of and consistency with applicable laws and	Inspected the policies and procedures and the service level agreements to determine that the	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		regulations, defined commitments, service-level agreements, and other contractual requirements.	entity's policies included procedures regarding the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	
		Policies and procedures are in place to assign responsibility and accountability for system security, availability, and confidentiality.	Inspected the security policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system security, availability, and confidentiality.	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.
		System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.	Inspected the Kaseya metrics tracking reports to determine that system downtime and operations issues were monitored.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor and record performance criteria for critical *designDATA* 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 designDATA server and network equipment.	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A third party enterprise monitoring application is used to monitor and record performance criteria for contracted *client* server and network equipment.	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.	No exceptions noted.
		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.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		All designDATA network operations center personnel are equipped with smart phones for use in the network and server monitoring alert process.	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.	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.
		Documented backup procedures are in place for company systems deemed critical by management, to guide personnel in performing backup system tasks.	Inspected documented backup procedures to determine that documented backup procedures are in place for critical designDATA systems.	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.5	Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	Documented backup procedures are in place for *customer* system backups performed by designDATA.	Inspected documented backup procedures to determine that documented backup procedures are in place for critical customer systems.	No exceptions noted.
		Data backups of contracted *customer* application components and databases are performed according to the timing reflected in the customer contract.	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.	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 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.
		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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.	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.
		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.	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.	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.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1	The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inquired of management regarding risk assessment to determine that procedures were in place to assess risks on a periodic basis.	No exceptions noted.
			Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	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 the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	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, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	No exceptions noted.
		A formal data security risk assessment is performed on an annual basis. Risks related to	Inspected the most recent risk assessment documentation to	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		handling data that are identified are evaluated and are formally documented, along with mitigation strategies, for management review.	determine that a formal data security risk assessment was performed during the review period and that identified risks were formally documented for management review.	
		Documented policies and procedures are in place to guide personnel when performing the risk assessment process.	Inspected risk assessment policies and procedures to determine that documented policies and procedures are in place to guide personnel when performing the risk assessment process.	No exceptions noted.
		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 any regulatory compliance or operational trends affecting the services provided.	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.	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.
			Observed redundant system infrastructure and the network configuration documentation to confirm server redundancy for critical production applications.	No exceptions noted.
		Redundant architecture is built into server infrastructure, including, but not limited to the:	Observed the redundant system infrastructure components to	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		• Network interface cards (NICs) • Power supplies • RAID-5 storage.	determine that redundant architecture was built into certain aspects of the systems infrastructure.	
		Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.	Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
			Inspected a judgmental sample of 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.	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.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inquired of management regarding risk assessment to determine that procedures were in place to assess risks on a periodic basis.	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	activities; and updates the controls, as necessary.			
			Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	No exceptions noted.
		Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inquired of management regarding security policies to determine that the entity's system security policies were established and periodically reviewed and approved by the director.	No exceptions noted.
			Inspected the policies and procedures manual to determine that the entity's system security policies were established.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.
		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.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and designDATA network.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.	No exceptions noted.
		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.	Inspected the network diagram to determine that multiple firewalls are setup for redundancy.	No exceptions noted.
			Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.	No exceptions noted.
		Firewall configurations filter internet traffic based on content and destination site address. The configurations include: • 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 certain destinations. All unused ports on the firewall are blocked. • The firewall is configured to deny all traffic that is not specifically authorized in the rule set.	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.	No exceptions noted.
			Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			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.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.	No exceptions noted.
		designDATA actively utilizes the following firewall features for protection at the perimeter of the network and between network segments: • Stateful packet inspection • IPSec/SSL VPN • Intrusion Detection and Prevention • Advance Threat Protection • Logging and • Reporting.	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.	No exceptions noted.
		Management maintains insurance coverage to protect against dishonest acts that may be committed by personnel.	Inspected insurance coverage policy declarations page to determine that management maintained insurance coverage to protect against dishonest acts by personnel.	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.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC4.0 - COMMON CRITERIA RELATED TO MONITORING OF CONTROLS

The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Security, availability, and confidentiality policies and procedures are in place and periodically reviewed by a designated individual or group.	Inquired of management regarding security, availability, and confidentiality policies to determine that the entity's system security, availability, and confidentiality policies were established and periodically reviewed and approved by the director.	No exceptions noted.
			Inspected the policies and procedures manual to determine that the entity's system security, availability, and confidentiality policies were established.	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.
		System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.	Inspected the Kaseya metrics tracking reports to determine that system downtime and operations issues were monitored.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor and record performance criteria for critical *designDATA* 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 designDATA server and network equipment.	No exceptions noted.

CC4.0 - COMMON CRITERIA RELATED TO MONITORING OF CONTROLS

The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A third party enterprise monitoring application is used to monitor and record performance criteria for contracted *client* server and network equipment.	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.	No exceptions noted.
		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.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.
		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.	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.	No exceptions noted.
			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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Users are required to authenticate via a unique user ID and password before being granted access to designDATA internal network domain.	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.	No exceptions noted.
		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.	Inquired of management to determine that management has authorized specific personnel to administer information security within the internal network domain, and has segregated duties.	No exceptions noted.
			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.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has segregated specific duties within the production environment for administering critical areas such as: • Network administration • Systems (including Active Directory) administration.	Inspected access rights listing to determine that management has segregated specific duties within the production environment for administering critical areas.	No exceptions noted.
		Production database and application server operating system account policies are controlled by the default domain group policy.	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.	No exceptions noted.
			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.	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.
		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.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and designDATA network.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.	No exceptions noted.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	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.
		Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	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.	Exception noted - During testing, a previously terminated employee was found to have access rights in system. Management response - Access rights for the terminated employee were immediately disabled and steps taken to improve control to ensure rights disabled consistently.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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.	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.	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.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	Users are required to authenticate via a unique user ID and password before being granted access to designDATA internal network domain.	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.	No exceptions noted.
		Internal network domain (default domain) passwords must conform to the following requirements: • Enforce password history • Maximum password age • Minimum password length • Complexity requirements.	Inspected the network authentication configurations to determine that network domain passwords must conform to stated requirements.	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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.	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.	No exceptions noted.
		Production database and application server operating system account policies are controlled by the default domain group policy.	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.	No exceptions noted.
			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.	No exceptions noted.
		The firewall requires two factor authentication before administrative access to the firewall system is allowed.	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.	No exceptions noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the	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.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
		Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	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.	Exception noted - During testing, a previously terminated employee was found to have access rights in system. Management response - Access rights for the terminated employee were immediately disabled and steps taken to improve control to ensure rights disabled consistently.
		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.	Inquired of management to determine that management has authorized specific personnel to administer information security within the internal network domain, and has segregated duties.	No exceptions noted.
			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	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			administering critical areas such as network administration, and database management.	
		Management has segregated specific duties within the production environment for administering critical areas such as: • Network administration • Systems (including Active Directory) administration.	Inspected access rights listing to determine that management has segregated specific duties within the production environment for administering critical areas.	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.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	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.
		designDATA utilizes various third party data centers for housing critical production computer servers, applications, and networking equipment. The third party data centers have physical access controls in place to restrict access to authorized personnel only.	Inspected the most recent SOC audit reports for the third party data centers to determine that physical access controls are present at the facilities utilized by designDATA.	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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.	Inspected the internal memos documented to determine that designDATA management reviews the SOC audit reports of the various third party data centers annually.	No exceptions noted.
CC5.6	Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	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.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and designDATA network.	No exceptions noted.
			Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.	No exceptions noted.
		The firewall requires two factor authentication before administrative access to the firewall system is allowed.	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.	No exceptions noted.
		All firewall administrator accounts have been changed from their default passwords.	Inspected the administrator account password configurations to determine that all firewall administrator accounts have been changed from their default passwords.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

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.	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.
			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.
		Hardware and software based firewalls and routers are placed at all network perimeter and third-party entry points to designDATA networks.	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	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			all network perimeter and third party entry points to designDATA networks.	
			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.	No exceptions noted.
		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.	Inspected the network diagram to determine that multiple firewalls are setup for redundancy.	No exceptions noted.
			Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.	No exceptions noted.
		Firewall configurations filter internet traffic based on content and destination site address. The configurations include: • 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 certain destinations. All unused ports on the firewall are blocked. • The firewall is configured to deny all traffic that is not specifically authorized in the rule set.	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.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.	No exceptions noted.
			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.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.	No exceptions noted.
		designDATA actively utilizes the following firewall features for protection at the perimeter of the network and between network segments: • Stateful packet inspection • IPSec/SSL VPN • Intrusion Detection and Prevention • Advance Threat Protection • Logging and • Reporting.	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.	No exceptions noted.
		Network administrators harden servers by enabling only necessary operating system services and roles, and factory default configurations are changed as appropriate: • Non-essential default accounts are turned off • Non-essential services are turned off • FTP access is disabled for non-FTP	Inquired of management to determine that network administrators harden servers by enabling only necessary operating system services and roles.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		servers • Security event logging is enabled.		
		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.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the security 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.
		The backup application encrypts the backup data for storage utilizing AES 256 bit encryption.	Inspected the control panel encryption settings to determine that the backup application encrypts the backup data for storage.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	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.
		Third party antivirus software is installed on certain designDATA servers (endpoint	Inquired of management to determine that third party antivirus	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		protection).	software is installed on all designDATA servers.	
			Inspected antivirus software installed on judgmental sample of designDATA servers to determine that antivirus software is installed on all designDATA servers.	No exceptions noted.
		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 every 4 hours.	Inspected the antivirus system's update settings to determine that a central server monitored for updates to antivirus definitions every four hours.	No exceptions noted.
			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.	No exceptions noted.
			Inspected the antivirus settings for frequency that updates are pulled to production servers to determine that updates were pulled to specific production servers every 4 hours.	No exceptions noted.
		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 SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

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

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1	Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	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.
			Inspected the monitoring application to determine that a scan schedule is utilized to monitor patch releases, and distribute patches to relevant devices.	No exceptions noted.
		designDATA IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.	Inspected a sample of informational service communications to determine that IT personnel utilize security issue monitoring services.	No exceptions noted.
			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.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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 (see below.)	Inspected the third party automated backup system to determine that automated backup systems are utilized to perform scheduled system backups.	No exceptions noted.
		Systems that are backed up include: • SQL servers • Exchange servers • Active directory servers • Application servers.	Inspected list of servers configured to be backed up to disk to determine that the enumerated servers are backed up.	No exceptions noted.
		Veeam is utilized to create tape backups of Veeam disk-to-disc backup jobs. The backup jobs are created and scheduled manually by authorized personnel.	Inspected judgmental sample of manual backup scheduling to determine that backup jobs are created and scheduled by authorized personnel.	No exceptions noted.
		Monthly full backups are performed of critical company data such as critical application and database components. Logs are used to record backup activity.	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.	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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	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 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.
		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.
		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.	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.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Helpdesk calls are entered into the ticketing system and call tracking utility and given a ticket number. • 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.	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.	No exceptions noted.
			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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1	The entity's commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	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.	Observed and 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.
			Inspected authentication policies and configurations for the production servers and administrative rights.	No exceptions noted.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	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.
		A ticketing system is utilized to manage systems infrastructure issues and changes.	Inspected a judgmental sample of logs from the Connectwise ticketing	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Tickets are assigned to support personnel based on the nature of the ticket.	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.	
		A standard hardware build is utilized for installation and maintenance of certain critical designDATA servers.	Inspected the standard hardware build procedures for certain designDATA servers to determine that a standard hardware build is utilized for certain critical designDATA servers.	No exceptions noted.
		A standard vHost template for virtualized environments is utilized for installation and maintenance of certain critical designDATA and customer virtual machines.	Inspected the vHost configurations to determine that a standard template is used for installation and maintenance of certain critical designDATA virtual machines.	No exceptions noted.
		Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.	Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
			Inspected a judgmental sample of 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.	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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.
			Inspected the monitoring application to determine that a scan schedule is utilized to monitor patch releases, and distribute patches to relevant devices.	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.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.	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 operating effectiveness of controls are identified during system operation and monitoring.	No exceptions noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.	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.

MATRIX 1 CRITERIA COMMON TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY PRINCIPLES

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

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 guide personnel regarding testing, evaluating, and authorizing system components before implementation.	Inspected the policies and procedures related to testing, evaluating, and authorizing before implementation of components.	No exceptions noted.
		Infrastructure changes and patches to third party applications are tested by the technical support department being applied to production servers.	Inquired of management to determine that infrastructure changes tested by the technical support department after hours before being introduced to production servers.	No exceptions noted.
			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.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Policies and procedures are in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	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.	No exceptions noted.
		Policies and procedures are in place for identifying and documenting the system availability and related security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system availability and related security policies were established.	No exceptions noted.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Policies and procedures are in place to guide personnel regarding the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	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, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	No exceptions noted.
		designDATA utilizes various third party data centers for housing certain critical production computer servers, applications, and networking equipment. The environmental controls at the third party data centers are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Inspected the most recent SOC audit reports for the third party data centers to determine that environmental access controls are present at the facilities utilized by designDATA.	No exceptions noted.
		designDATA management reviews the SOC audit reports of the various third party data	Inspected the internal memos documented to determine that	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		centers annually and documents the results of the reviews of the SOC audit reports in a memo.	designDATA management reviews the SOC audit reports of the various third party data centers annually.	
		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 disruption. In the event of failure of one or more lines, the enterprise monitoring system sends alert notifications.	Inspected the internet connection failover alert configurations in the router interface to determine that multiple internet connections provide active-active redundancy, and that in the event of failure of one or more lines, the enterprise monitoring system sends alert notifications.	No exceptions noted.
		designDATA utilizes fully redundant routing and switching equipment for its core networking infrastructure.	Inspected network diagram to determine that designDATA utilizes fully redundant routing and switching equipment for its core networking infrastructure.	No exceptions noted.
		Documented backup procedures are in place for company systems deemed critical by	Inspected documented backup procedures to determine that	No exceptions noted.

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		management, to guide personnel in performing backup system tasks.	documented backup procedures are in place for critical designDATA systems.	
		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: 5. Production data 6. Backup copy on Exagrid appliance 7. Replicated copy at redundant data center 8. Monthly copy to tape (see below.)	Inspected the third party automated backup system to determine that automated backup systems are utilized to perform scheduled system backups.	No exceptions noted.
		The backups are asynchronous. • 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.	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.	No exceptions noted.
		The retention period for backup data is 21 restore points.	Inspected a judgmental sample of backup data jobs to determine that the retention period is 21 restore points.	No exceptions noted.
		Systems that are backed up include: • SQL servers • Exchange servers • Active directory servers • Application servers.	Inspected list of servers configured to be backed up to disk to determine that the enumerated servers are backed up.	No exceptions noted.
		Veeam is utilized to create tape backups of Veeam disk-to-disc backup jobs. The backup jobs are created and scheduled manually by authorized personnel.	Inspected judgmental sample of manual backup scheduling to determine that backup jobs are created and scheduled by authorized personnel.	No exceptions noted.

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Monthly full backups are performed of critical company data such as critical application and database components. Logs are used to record backup activity.	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.	No exceptions noted.
		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.	Inquired of management to determine that multiple backup tapes are used in rotation as backup media.	No exceptions noted.
		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.	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.	No exceptions noted.
		Backup media are rotated off-site according to a formal rotation schedule.	Inspected the rotation schedule for backup media to determine that backup media are rotated off-site according to a formal rotation schedule.	No exceptions noted.
		Manual backup jobs are monitored for failure by authorized personnel.	Observed backup monitoring process to determine that backup jobs are monitored for failure by authorized personnel.	No exceptions noted.
		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.	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.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			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.	No exceptions noted.
		The backup applications generate and maintain **logs**, which specify the data backup processes are completed, and success/failure status of each process.	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.	No exceptions noted.
		Management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.	Inquired of management to determine that management performs systematic reviews of the backup application and logs to detect abnormalities in the backup process.	No exceptions noted.
			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.
		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.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system’s availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	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.
		Policies and procedures are in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.	Inspected the policies and procedures and service level agreement s 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.	No exceptions noted.
		Management periodically performs restorations of backup data at customer request, which serves to verify the success of backup processes and employee readiness.	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.	No exceptions noted.
			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.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY PRINCIPLE

Confidentiality Principle and Criteria Table
The confidentiality principle refers to the system's ability to protect information designated as confidential as committed or agreed by the organization.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	Policies and procedures are in place to ensure that confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.	Observed and inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.	No exceptions noted.
		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.	Observed and 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.
			Inspected authentication policies and configurations for the production servers and administrative rights.	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	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY PRINCIPLE

Confidentiality Principle and Criteria Table
The confidentiality principle refers to the system’s ability to protect information designated as confidential as committed or agreed by the organization.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.		signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	
		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.
		Procedures have been implemented related to confidentiality of inputs, data processing, and outputs which are consistent with the documented confidentiality policies.	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.	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 data processing and storage.	No exceptions noted.
			Inspected encryption policies to determine that encryption methods are in place and utilized for sensitive data processing and storage.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY PRINCIPLE

Confidentiality Principle and Criteria Table
The confidentiality principle refers to the system's ability to protect information designated as confidential as committed or agreed by the organization.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the security 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.
		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.	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	No exceptions noted.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	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.	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	No exceptions noted.
		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.	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.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY PRINCIPLE

Confidentiality Principle and Criteria Table
The confidentiality principle refers to the system's ability to protect information designated as confidential as committed or agreed by the organization.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	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.	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.	No exceptions noted.
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	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.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	Policies and procedures are in place to communicate retention periods for confidential information maintained by designDATA. Procedures are in place to: • Automatically delete confidential information in accordance with specific retention requirements;	Inspected designDATA's retention policies for confidential information to determine that the policies included procedures to: • Automatically delete confidential information in accordance with specific	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY PRINCIPLE

Confidentiality Principle and Criteria Table

The confidentiality principle refers to the system's ability to protect information designated as confidential as committed or agreed by the organization.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		- 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.	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.	
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Policies and procedures are in place to communicate designDATA's destruction policy for confidential information.	Inspected the destruction policy to determine that policies and procedures are in place to communicate designDATA's destruction policy for confidential information.	No exceptions noted.
		The entity: - 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; - 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	Inquired of management to determine that the entity: - 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; - erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example,	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CONFIDENTIALITY PRINCIPLE

Confidentiality Principle and Criteria Table
The confidentiality principle refers to the system's ability to protect information designated as confidential as committed or agreed by the organization.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		• documents the disposal of confidential information.	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.	

END OF REPORT