designDATA

Managed Services | IT Consulting | Data Center

GENERAL CONTROLS SUPPORTING THE DATA CENTER AND MANAGED SERVICES

SOC 1 - Type II Audit Report

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of the Controls

For the Period June 1, 2016 to May 31, 2017

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 designDATA's Description of Its Data Center and Managed Services and Systems and the Suitability of the Design and Operating Effectiveness of Controls

To: designDATA

Scope

We have examined designDATA's (designDATA) description of its data center and managed services and systems entitled "Description of the Service Organization's System Provided by Management" for processing user entities' transactions throughout the period June 1, 2016 to May 31, 2017 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertions by the Service Organization's Management" (assertion). The controls and control objectives included in the description are those that management of designDATA believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the data center and managed services and systems that are not likely to be relevant to user entities' internal control over financial reporting.

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

designDATA uses a third party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description includes only the control objectives and related controls of designDATA and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by designDATA can be achieved only if complementary subservice organization controls assumed in the design of designDATA's controls are suitably designed and operating effectively, along with the related controls at designDATA. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service organization's responsibilities

In Section 2, designDATA has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. 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, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period June 1, 2016 to May 31, 2017. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent limitations

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

Description of tests of controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in designDATA's assertion -

a. the description fairly presents the data center and managed services and systems that were designed and implemented throughout the period June 1, 2016 to May 31, 2017.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period June 1, 2016 to May 31, 2017 and user entities and subservice organizations applied the complementary controls assumed in the design of designDATA's controls throughout the period June 1, 2016 to May 31, 2017.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period June 1, 2016 to May 31, 2017 if complementary user entity and subservice organization controls assumed in the design of designDATA's controls operated effectively throughout the period June 1, 2016 to May 31, 2017.

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 management of designDATA, user entities of designDATA's data center and managed services and systems during some or all of the period June 1, 2016 to May 31, 2017, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

The Moore Group CPA, LLC

Nashua, NH
July 10, 2017

SECTION 2

ASSERTIONS BY THE SERVICE ORGANIZATION'S MANAGEMENT

Assertion of the Management of designDATA

The Moore Group CPA, LLC
131 Daniel Webster Highway, Suite 618
Nashua, NH 03060

We have prepared the description of designDATA's data center and managed services and systems entitled "Description of the Service Organization's System Provided by Management" for processing user entities' transactions throughout the period June 1, 2016 to May 31, 2017 (description) for user entities of the system during some or all of the period June 1, 2016 to May 31, 2017, and their auditors who audit and report on such user entities' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatements of user entities' financial statements.

designDATA uses a third party data center (subservice organization) to house its critical production computer servers, applications, and networking equipment. The description includes only the control objectives and related controls of designDATA and excludes the control objectives and related controls of the third party data center. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

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

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

1) The description fairly presents the data center and managed services and systems made available to user entities of the system during some or all of the period June 1, 2016 to May 31, 2017 for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    a) Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

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

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

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

iv) How the system captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for user entities.

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

vii) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.

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

b) Includes relevant details of changes to the data center and managed services and systems during the period covered by the description.

c) Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the data center and managed services and systems that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period June 1, 2016 to May 31, 2017 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of designDATA's controls throughout the period June 1, 2016 to May 31, 2017. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management.

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

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

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY 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.

Description of Services Provided

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

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

- A physical location outside of the immediate metropolitan area
- High level of premise security including 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.

Facilities and Data Flow

designDATA utilizes a secure third party datacenter known as SAVVIS, a CenturyLink Company, located in Sterling, Virginia. This data center continues to provide co-location services to top tier customers for critical production servers and systems. SAVVIS had a SOC 2 report for the period October 1, 2015 to September 30, 2016. Although the scope of this audit does not include the controls of SAVVIS, a summary of its physical and environmental security controls are outlined as described therein, in Section 5 of this report.

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, 2016 to December 31, 2016. Although the scope of this audit does not include the controls of BYTEGRID, a summary of its physical and environmental security controls are outlined as described therein, in Section 5 of this report.

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.

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. 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.

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.

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.

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.

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.

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.

Organizational Structure and Assignment of Authority and Responsibility

designDATA's organizational 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 organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. designDATA has developed an organizational structure suited to its needs. This organizational 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 set objectives and that the chosen 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.

designDATA's control objectives 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 control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of designDATA's description of controls.

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.
- Organizational 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.

DISCLOSURES OF RELEVANT INFORMATION

Significant Changes During the Review Period

There were no significant changes to the control environment during the review period.

Subsequent Events

No material events occurred subsequent to the period covered by management's description of the service organization's system up to the date of the service auditor's report that could have a significant effect on management's assertion.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of the internal audit function in preparing this report.

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 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 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Integrity and Ethical Values		
1.1	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.
1.2	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.
1.3	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.
1.4	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.	Inquired of management to determine that 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.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.5	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.
1.6	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.
1.7	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.
	Commitment to Competence		
1.8	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.
1.9	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.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.10	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.
		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.
1.11	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.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.12	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.
	Board of Directors Participation		
1.13	A board of directors **oversees management activities**.	Inquired of management regarding the board of directors to determine that a board of directors was in place to oversee management activities.	No exceptions noted.
		Inspected the listing of the board of director members to determine that a board of directors was in place.	No exceptions noted.
1.14	The board of directors **meets on a semi-annual basis**.	Inquired of management to determine that a board of directors meets semi-annually.	No exceptions noted.
		Inspected the most recent BOD meeting agenda.	No exceptions noted.
1.15	designDATA utilizes a **third party financial services firm** to prepare annual tax returns.	Inquired of management to determine that designDATA utilizes a third party financial services firm to prepare annual tax returns.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Management Philosophy and Operating Style		
1.16	Management is guided by designDATA's corporate **mission statement** in determining the implementation of corporate goals and operational activities to meet them.	Inspected designDATA's corporate mission statement to determine that management is guided by designDATA's corporate mission statement in determining the implementation of corporate goals operational activities to meet them.	No exceptions noted.
1.17	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.
1.18	**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.	Inquired of management to determine that management meetings were held on a regular basis to discuss operational and customer related issues.	No exceptions noted.
	Organizational Structure, and Assignment of Authority and Responsibility		
1.19	**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.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		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.
1.20	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 close oversight maintained by the CEO.	No exceptions noted.
1.21	designDATA's **operating goals and objectives are communicated** to the entire organization during regular staff meetings, employee performance reviews, and other written communications.	Inquired of management regarding communication of designDATA's operating goals and objectives to employees of organization to determine that they are communicated to the entire organization.	No exceptions noted.
		Inspected a judgmental sample of written company communications to determine that designDATA's operating goals and objectives are communicated to the entire organization.	No exceptions noted.
1.22	designDATA provides an **employee orientation program** that communicates organizational structure and responsibility, company and departmental objectives, and relationships between departments and personnel.	Inquired of management regarding the employee orientation program to determine that organizational structure, responsibility, company and departmental objectives and relationships between departments are communicated to employees during the orientation.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected employee orientation documentation to determine that organizational structure, responsibility, company and departmental objectives and relationships between departments are communicated to employees during the orientation.	No exceptions noted.
1.23	designDATA has established a **segregation of duties process**, which is based upon changes and recommendations from management.	Inquired of management regarding segregation of duties process.	No exceptions noted.
		Inspected the organization chart to determine that designDATA has established a segregation of duties process.	No exceptions noted.
	Human Resource Policies and Practices		
1.24	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.	Inspected the hiring guidelines and procedures to determine that such documentation guides the hiring process.	No exceptions noted.
		Inspected Paychex customer portal with the HR provider to determine that designDATA utilizes the services of an independent, outsourced HR services provider.	No exceptions noted.
1.25	Human Resources management utilizes an **onboarding 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.	Inspected a judgmental sample of within ConnectWise onboarding tickets used for employees hired during the review period to determine that HR management utilizes an onboarding checklist for the employees and that the checklist is retained in the employee files.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.26	Each employee undergoes monthly informal one-on-one and annual **performance reviews** with management. During these reviews, management reinforces and updates professional development plans for each employee.	Inquired of management to determine that each employee undergoes monthly informal one-on-one and annual performance reviews with management.	No exceptions noted.
1.27	Management has established **employee termination procedures** that guide the termination process.	Inspected the employee termination procedures, to determine that they are used to guide the termination process.	No exceptions noted.
1.28	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.

MATRIX 2 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	THIRD PARTY HOSTING FACILITIES		
2.1	designDATA utilizes the services and controls of various third party data centers for housing certain critical production computer servers, applications, and networking equipment. These data centers are: • ByteGrid • CenturyLink.	Inspected Service Level Agreements with the various data centers/co-location facilities.	No exceptions noted.
	A summary of the various data centers' physical and environmental security controls are described in Section 5 as included in the most recent SOC report for each data center.	Inspected the most recent SOC audit report for each data center.	No exceptions noted.
2.2	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.

MATRIX 3 ENVIRONMENTAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	THIRD PARTY HOSTING FACILITIES		
3.1	designDATA utilizes the services and controls of various third party data centers for housing certain critical production computer servers, applications, and networking equipment. These data centers are: • ByteGrid • CenturyLink.	Inspected Service Level Agreements with the various data centers/co-location facilities.	No exceptions noted.
	A summary of the various data centers' physical and environmental security controls are described in Section 5 as included in the most recent SOC report for each data center.	Inspected the most recent SOC audit report for each data center.	No exceptions noted.
3.2	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.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of designDATA's and customers' critical files, storage of designDATA's and contracted customer's data, and retention of designDATA's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
4.1	Documented **backup procedures** are in place for company systems deemed critical by management, to guide personnel in performing backup system tasks. **Disk-to-Disk Image-Based Backups**	Inspected documented backup procedures to determine that documented backup procedures are in place for critical designDATA systems.	No exceptions noted.
4.2	**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.
4.3	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.
4.4	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.
4.5	**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.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of designDATA's and customers' critical files, storage of designDATA's and contracted customer's data, and retention of designDATA's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Manual Backup to External Tapes (Veeam Application)		
4.6	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.
4.7	**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.
4.8	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.
4.9	**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.
4.10	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.
4.11	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.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of designDATA's and customers' critical files, storage of designDATA's and contracted customer's data, and retention of designDATA's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Backup of Customer Applications and Data		
4.12	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.
4.13	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.
	Backup Monitoring		
4.14	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.
4.15	**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.
		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.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of designDATA's and customers' critical files, storage of designDATA's and contracted customer's data, and retention of designDATA's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
4.16	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.
4.17	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.
4.18	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.
4.19	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 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.1	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.
5.2	**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.
5.3	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.
5.4	**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.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		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.
5.5	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.
	System Monitoring and Response		
5.6	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.
5.7	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.
5.8	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.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.9	**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.
5.10	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.
5.11	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.
5.12	designDATA provides network **operations center personnel** on a 24/7/365 basis for server and network performance monitoring.	Inquired of management to determine that designDATA network operations center personnel are provided on a 24/7/365 basis for server and network performance monitoring.	No exceptions noted.
		Observed server and network performance monitoring in network operations center to determine that designDATA provides network operations center personnel on a 24/7/365 basis for server and network performance monitoring.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Hardware and Maintenance		
5.13	A **ticketing system** is utilized to manage systems **infrastructure issues**. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the 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.
5.14	**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.
5.15	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.
5.16	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.
5.17	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 servers • Security event logging is enabled.	Inquired of management to determine that network administrators harden servers by enabling only necessary operating system services and roles.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.18	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.
5.19	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.
5.20	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.
5.21	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.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.22	**Redundant architecture** is built into server infrastructure, including, but not limited to the: • Network interface cards (NICs) • Power supplies • RAID-5 storage. **<u>Telecommunications (Internet) Connectivity</u>**	Observed the redundant system infrastructure components to determine that redundant architecture was built into certain aspects of the systems infrastructure.	No exceptions noted.
5.23	**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.
5.24	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.
5.25	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.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	OS and Software Patches: (designDATA Servers)		
5.26	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.
5.27	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.
	Anti-virus Software		
5.28	Third party **antivirus software** is installed on all designDATA servers **(endpoint protection).**	Inquired of management to determine that third party antivirus software is installed on all designDATA servers.	No exceptions noted.
		Inspected antivirus software installed on judgmental sample of designDATA servers to determine that antivirus software is installed on all designDATA servers.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.29	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.

MATRIX 6 INFORMATION SECURITY

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

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
6.1	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.
6.2	**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.
6.3	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.
6.4	**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.
6.5	Management periodically performs **internal security assessments,** including reviews of server logs and other critical items.	Inquired of management to determine that management periodically performs internal security assessments during the review period.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

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

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
6.6	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.
6.7	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.	No exceptions noted.
6.8	Management has **segregated specific duties** within the production environment for administering critical areas such as: • Network administration • Systems (including Active Directory) administration. **Internal Network Domain –** Network Authentication Controls Via Windows Active Directory	Inspected access rights listing to determine that management has segregated specific duties within the production environment for administering critical areas.	No exceptions noted.
6.9	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.

MATRIX 6 INFORMATION SECURITY

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

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
6.10	Internal network domain (default domain) **passwords must conform** to the following requirements: • Enforce password history • Maximum password age • Minimum password length.	Inspected the network authentication configurations to determine that network domain passwords must conform to stated requirements.	No exceptions noted.
6.11	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. **Internal Network Domain –** Network Access and Monitoring Controls	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.
6.12	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.

MATRIX 6 INFORMATION SECURITY

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

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
6.13	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.
6.14	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.
6.15	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 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to designDATA's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Firewall System Administration		
7.1	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.
7.2	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.
7.3	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.
7.4	Administrative **access** 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.
7.5	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.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to designDATA's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.6	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. **Firewall Utilization**	Inspected the firewall system configuration and sample firewall system logs to determine that firewalls are configured to log all blocked packets.	No exceptions noted.
7.7	**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.
7.8	**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 all network perimeter and third party entry points to designDATA networks.	No exceptions noted.
		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.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to designDATA's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.9	**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.
7.10	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.
		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.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to designDATA's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		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.
7.11	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.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MATRIX 8 SERVICES AND CONTROLS PROVIDED BY THIRD PARTY DATA CENTERS.

designDATA utilizes the services and controls of the SAVVIS-CenturyLink data centers for housing critical production computer servers, applications, and networking equipment of designDATA and customers. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data Center Described by the Service Organization	Resources utilized by the Service Organization to provide this Description
	Savvis-CenturyLink Data Center *Sterling, VA*	
	Physical Security	
8.1	Physical access control systems are in place to restrict access to and within the data centers housing the offline storage, backup data, systems, and media to properly authorized individuals.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.2	Data center badge access requests for CenturyLink employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.3	Physical access is revoked for employees as a component of the employee termination process.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
	Environmental Security	
8.4	Enterprise monitoring applications are utilized to monitor for attributes that include, but are not limited to, the following: • System performance and availability • Physical and environmental security alarms.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.

MATRIX 8 SERVICES AND CONTROLS PROVIDED BY THIRD PARTY DATA CENTERS.

designDATA utilizes the services and controls of the SAVVIS-CenturyLink data centers for housing critical production computer servers, applications, and networking equipment of designDATA and customers. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data Center Described by the Service Organization	Resources utilized by the Service Organization to provide this Description
8.5	The monitoring applications notify operations personnel via onscreen alerts when predefined thresholds are exceeded on monitored systems.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.6	The data centers are equipped with the following environmental protection equipment: data centers to determine that the • Fire detection and suppression systems • HVAC units • Generators suppression systems • Electrical systems.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.7	Facilities personnel retain the inspection report completed by third party specialists to evidence the inspection and maintenance of the following on at least an annual basis: • Fire detection and suppression equipment • HVAC units • Generators • Electrical systems.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.8	Enterprise monitoring applications are utilized to monitor for attributes that include, but are not limited to, the following: • System performance and availability • Physical and environmental security alarms.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.9	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.

MATRIX 8 SERVICES AND CONTROLS PROVIDED BY THIRD PARTY DATA CENTERS.

designDATA utilizes the services and controls of the SAVVIS-CenturyLink data centers for housing critical production computer servers, applications, and networking equipment of designDATA and customers. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data Center Described by the Service Organization	Resources utilized by the Service Organization to provide this Description
8.10	Certain in-scope systems have redundancy to prevent processing delays should the primary infrastructure become unavailable.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.11	HVAC systems are in place at each data center.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.
8.12	Third party specialists inspect HVAC systems and water detection sensors, as applicable, on an annual basis.	SOC 2 report for Savvis, A CenturyLink Company, for the period October 1, 2015 to September 30, 2016.

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THIRD PARTY DATA CENTERS.

designDATA utilizes the services and controls of a ByteGrid Holdings LLC data center for housing critical production computer servers, applications, and networking equipment of designDATA and customers. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data Center Described by the Service Organization	Resources utilized by the Service Organization to provide this Description
	ByteGrid Holdings LLC Datacenter *Metro Washington DC Campus, Silver Spring, MD* **Physical Security**	
9.1	Documented physical access policies and procedures are in place to guide personnel in physical security practices.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.2	A badge access system is in place to restrict access to authorized personnel.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.3	Control self-assessments that include physical access reviews are performed on a quarterly basis.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.4	Access to system resources is revoked as a component of the termination process.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.5	A video surveillance system is in place with footage retained for at least 90 days.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.6	Visitors to the data centers are required to sign in and be escorted by an authorized data center employee.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.7	A visitor access log is used which identifies the visitor name, company name, arrival and departure date and sponsor during the visit.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THIRD PARTY DATA CENTERS.

designDATA utilizes the services and controls of a ByteGrid Holdings LLC data center for housing critical production computer servers, applications, and networking equipment of designDATA and customers. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data Center Described by the Service Organization	Resources utilized by the Service Organization to provide this Description
9.8	Mantraps or other physical devices are used for controlling accessing highly sensitive facilities.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
	Environmental Security	
9.9	Environmental protections have been installed and include the followin • HVAC • UPS • Generator backups in the event of power failure • Redundant communication lines • Smoke detectors • Fire extinguishers • Fire suppression system.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.10	Production equipment within the colocation areas of the data center facilities is placed on racks to protect infrastructure from localized flooding.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.11	The data center facilities are equipped with raised flooring to elevate equipment and help facilitate cooling.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.12	The data center facilities are equipped with leak detection systems to detect water in the event of a flood or water leakage.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.13	Operations personnel monitor the status of environmental protections.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THIRD PARTY DATA CENTERS.

designDATA utilizes the services and controls of a ByteGrid Holdings LLC data center for housing critical production computer servers, applications, and networking equipment of designDATA and customers. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data Center Described by the Service Organization	Resources utilized by the Service Organization to provide this Description
9.14	Environmental protections receive maintenance on at least an annual basis.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.15	Shift turnover reports document environmental system monitoring performed during each shift.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.16	Disaster response plans have been developed and are updated annually.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.
9.17	Disaster recovery plans are tested on an annual basis.	SOC 2 plus HiTrust report for ByteGrid Holdings, LLC for the period January 1, 2016 to December 31, 2016.

END OF REPORT