DATAPIPE®

a rackspace® company

REPORT ON DATAPIPE, INC.'S DESCRIPTION OF ITS MANAGED CLOUD AND HOSTING SERVICES AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD APRIL 1, 2017 TO MARCH 31, 2018

SOC for Service Organizations - SOC 2 Type 2

COALFIRE® CONTROLS

TABLE OF CONTENTS

SECTION 1

SECTION 2

SECTION 3

SECTION 4

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Datapipe, Inc. ("Datapipe")

SCOPE

We have examined the description in Section 3 titled "Description of Datapipe, Inc.'s Managed Cloud and Hosting Services for the Period April 1, 2017 to March 31, 2018" (description) based on the criteria set forth in paragraph 1.26 of the 2015 AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability and confidentiality principles set forth in TSP Section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016) (applicable trust services criteria), throughout the period April 1, 2017 to March 31, 2018. The controls included in the description are those that management of Datapipe believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of Datapipe's Managed Cloud and Hosting Services that are not likely to be relevant to meeting the applicable trust services criteria. The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Datapipe'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.

As indicated in the description, Datapipe uses service organizations (subservice organizations) for data center colocation services. The description indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of Datapipe's controls are suitably designed and operating effectively, along with the related controls at Datapipe. The description presents Datapipe's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organizations. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

SERVICE ORGANIZATION'S RESPONSIBILITIES

In Section 2, Datapipe has provided its assertion titled "Assertion of the Management of Datapipe, Inc." (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Datapipe is responsible for selecting the applicable trust services principles addressed by the engagement; preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; identifying any applicable trust services criteria relevant to the principles addressed by the engagement that have been omitted from the description and explaining the reason for omission; designing, implementing, and documenting the controls that are suitably designed and operating effectively to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

SERVICE AUDITOR'S RESPONSIBILITIES

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

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

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period April 1, 2017 to March 31, 2018.
- assessing the risks that the description is not fairly presented based on the description criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- evaluating the overall presentation of the description, the suitability of the applicable trust services criteria stated therein, and the 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 users and may not, therefore, include every aspect of the system that each individual user may consider important in its own particular environment. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

OPINION

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

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

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period April 1, 2017 to March 31, 2018 and user entities applied the complementary user entity controls assumed in the design of Datapipe's controls throughout the period April 1, 2017 to March 31, 2018, and the subservice organizations applied the complementary controls assumed in the design of Datapipe's controls throughout the period April 1, 2017 to March 31, 2018.

c. the controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period April 1, 2017 to March 31, 2018 if user entities applied the complementary user entity controls assumed in the design of Datapipe's controls, and those controls operated effectively throughout the period April 1, 2017 to March 31, 2018 and if the complementary subservice organization controls assumed in the design of Datapipe's controls operated effectively throughout the period April 1, 2017 to March 31, 2018.

DESCRIPTION OF TESTS OF CONTROLS

The specific controls we tested, the tests we performed, and the results of our tests are listed in Section 4, "Trust Services Security, Availability and Confidentiality Principles, Criteria, Related Controls and Tests of Controls" of this report.

RESTRICTED USE

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Datapipe; user entities of Datapipe's Managed Cloud and Hosting Services during some or all of the period April 1, 2017 to March 31, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

Coalfire Controls LLC

May 25, 2018
Louisville, Colorado

SECTION 2

DATAPIPE, INC.'S ASSERTION

Assertion of the Management of Datapipe, Inc. ("Datapipe")

We have prepared the description titled "Description of Datapipe's Managed Cloud and Hosting Services for the Period April 1, 2017 to March 31, 2018" (description), based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC $2^{®}$)* (description criteria). The description is intended to provide users with information about the Managed Cloud and Hosting Services, particularly system controls intended to meet the criteria for the security, availability and confidentiality principles set forth in *TSP section 100*, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria), throughout the period April 1, 2017 to March 31, 2018.

Datapipe uses subservice organizations, Equinix, TeleHouse, Global Switch, DataBank Holdings, Ltd. and Amazon Web Services (AWS), for colocation services. The description includes only the applicable trust services criteria and related controls of Datapipe and excludes the applicable trust services criteria and related controls of Equinix, TeleHouse, Global Switch, DataBank Holdings, Ltd. and AWS. The description also indicates that certain applicable trust services criteria specified in the description can be met 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 organizations.

The description indicates that the applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Datapipe's controls are suitably designed and operating effectively along with related controls at the service organization and the subservice 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 Managed Cloud and Hosting Services throughout the period April 1, 2017 to March 31, 2018 as it relates to controls that are likely to be relevant to meeting the applicable trust services criteria. Our assertion is based on the following description criteria:

    i. The description contains the following information:

        1) The types of services provided.

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

            - *Infrastructure*. The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
            - *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
            - *People*. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel and managers).
            - *Procedures*. The automated and manual procedures.
            - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

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

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

   a. how the information is provided or received and the role of the subservice organizations and other parties.

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

5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user entity controls contemplated in the design of the service organization's system.

6) Regarding the subservice organizations that are presented using the carve-out method

   a. the nature of the services provided by the subservice organizations.

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

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

8) Relevant details of changes to the service organization's system during the period covered by the description.

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

b. the controls stated in the description were suitably designed throughout the period April 1, 2017 to March 31, 2018 to meet the applicable trust services criteria, if the subservice organizations and user entities applied the complementary controls assumed in the design of Datapipe's controls throughout the period April 1, 2017 to March 31, 2018.

c. the controls stated in the description operated effectively throughout the period April 1, 2017 to March 31, 2018 to meet the applicable trust services criteria, if the subservice organizations and user entities applied the complementary controls assumed in the design of Datapipe's controls throughout the period April 1, 2017 to March 31, 2018.

____
Datapipe, Inc. Authorized Representative

Michael Bross, General Counsel ____________
Title

SECTION 3

DESCRIPTION OF DATAPIPE’S MANAGED CLOUD AND HOSTING SERVICES FOR THE PERIOD APRIL 1, 2017 TO MARCH 31, 2018

Datapipe, Inc. has used DC Section 200A, *2015 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, to prepare the description of its system.

OVERVIEW OF OPERATIONS

COMPANY BACKGROUND

Datapipe, Inc. ("Datapipe" or "the Company"), headquartered in Jersey City, New Jersey, is a global provider of managing and securing mission-critical information technology (IT) services, including cloud computing, infrastructure as a service, platform as a service, colocation and data centers, to businesses worldwide. Datapipe has over 800 employees and fifteen data centers operating worldwide in the following locations: New Jersey, California, Virginia, Missouri, Colorado, Texas, London, Amsterdam, Hong Kong, and Singapore.

SCOPE OF THIS REPORT

The security, availability, and confidentiality Trust Services Principles (TSP) are in scope for purposes of this report. The systems, locations and services that are in scope are as follows:

Systems

- Management Network - Secure Access Network for Transparent Administration (SANTA)
  - A secure isolated network used by authorized employees to remotely manage Client resources.
  - Accessible only to authorized employees by leveraging a SSL Two Factor VPN.
  - PCI compliant environment leveraging security best practices and Datapipe's enterprise security controls.
- Configuration Management Database (CMDB) - Datapipe One (DP1)
  - Includes ticketing, change management, incident management, and problem management.
- AWS Management – Cloud Management System (CMS) and Datapipe Access and Audit Control for the Cloud (DAAC)
  - Role-based access control platform for Datapipe support personnel management of AWS resources.
  - Accountability achieved with all system access and activities tied to Datapipe support user's unique account.
  - Leverages two-factor authentication for Datapipe employees via Single Sign On.
  - Employees' keys are stored in Secret Server and never exposed to the employees themselves.
  - Client administrative API keys are not required for Datapipe AWS console administration.
- PCI Community Cloud Platform (PCI vStrat)
  - PCI compliant platform leveraging security best practices and Datapipe's enterprise security controls.
  - Community based platform ensuring all guests perform payment card workloads.
  - A non-mixed mode policy ensures all guests are at the same security level.
  - Tenants on the PCI vStrat platform are logically isolated from all other tenants.

- Password Management / Password Vault
  - A role based password vaulting system used by Datapipe employees to securely access internal and external credentials.
  - Password check-in/check-out functionality ensure a credential is rotated after each use.
  - Leverages strong-cryptography and hardware security modules (HSM)

Locations

The data centers that are in scope for purposes of this report are listed in the table below. At certain locations, Datapipe leases dedicated space from third party data centers (subservice organizations).

Location	Datapipe Owned	Subservice Organization Owned	Subservice Organization
New Jersey One Facility: 200 Campus Drive, Somerset NJ 08873, United States	☑		
New Jersey Two Facility: 125 Belmont Drive, Somerset NJ 08873, United States	☑		
Silicon Valley One Facility: 150 South 1st Street, Suite 101, San Jose CA 95113, United States	☑		
AirWorld Technology, 10828 NW AirWorld Kansas City, MO 64153 United States	☑		
North Virginia One Facility: 21715 Filigree Court, Ashburn VA 20147, United States		☑	Equinix
London Two Facility: 8 Buckingham Avenue, Slough, SL1 4AX, United Kingdom		☑	Equinix
Hong Kong One Facility: 1 Wang Wo Tsai Street, Tsuen Wan, Hong Kong		☑	Equinix
Singapore Three Facility: 26A Ayer Rajah Crescent 139963, Singapore		☑	Equinix
Amsterdam Facility: Luttenbergweg 4 1101 EC, Amsterdam The Netherlands		☑	Equinix
Frankfurt Facility: Kruppstraße 121-127 60388, Frankfurt Germany		☑	Equinix
Hong Kong Two Facility: 2 Chun Yat Street, Tseung Kwan O Industrial Estate, Hong Kong		☑	TeleHouse

Location	Datapipe Owned	Subservice Organization Owned	Subservice Organization
Shanghai Two Facility: Qinqiao Road No. 368, Pudong District, Shanghai, 201206, China		☑	TeleHouse
London One Facility: 3 Nutmeg Lane, London, E14 2AX, United Kingdom		☑	Global Switch
DataBank, 400 S Akard St. Dallas, TX 75202 United States		☑	DataBank Holdings, Ltd.
Global		☑	Amazon Web Services (AWS)

The third-party data centers manage and operate a portion of data center services including aspects of physical safeguarding of IT infrastructure and environmental protections. At each third-party data center, Datapipe has created its own access control system to protect its suites. These suites are considered to be independent of the subservice organization's suites and can only be accessed by authorized Datapipe employees. Any employees of the subservice organizations or visitors that enter the suites are required to be escorted at all times. The scope of this report includes all physical security and environmental controls at the Datapipe-owned locations. For the third-party data centers, the scope of this report includes the physical security controls that are operated by Datapipe and excludes those physical security and environmental controls that are operated by the third-party data centers.

DESCRIPTION OF SERVICES PROVIDED

Managed Hosting

Datapipe offers different levels of managed services best-suited for each client's IT environment according to the level of complexity associated with system requirements, beginning with system monitoring and adding layers of increasing management support as needed. Datapipe offers various types of solutions, including: physical, cloud (managed AWS, PCI vStrat), and hybrid solutions, as well as Health Insurance Portability and Accountability Act (HIPAA) and PCI compliance security services.

Datapipe's day-to-day IT administration activities employ a dedicated security staff. Clients with heightened data security expectations who utilize Layer 3: Full Management services can add the Layer 4 Compliance Management suite of security services that satisfies many requirements of industry/regulatory standards, including HIPAA / Health Information Technology for Economic and Clinical Health (HITECH) and the Payment Card Industry's Data Security Standard (PCI DSS).

Layer 4 managed services can be applied to any system or network device. Additionally, Datapipe offers enterprise-level management of database software (MS SQL, MySQL, Oracle) as an add-on to system management services.

Implementation & Support Team

- Assigned account manager
- Network engineers
- Systems engineer
- Assigned service delivery manager
- Certified database administrators

Hardware Management

- Procurement of hardware
- Assembly of hardware
- Configuration of hardware
- Hardware sparing

Operating System Management

- Installation of operating system
- Configuration of operating system
- All operating system patches and upgrades
- Operating system optimization
- Operating system management
- 24x7x365 maintenance and support of supported operating systems

Network & Network Security Management

- Managed firewall services (with Virtual Private Network (VPN) capabilities)
- Firewall administration
- Managed client VPN services
- IP address allocation
- Domain name services (DNS) as required by the client

Application Management

- Installation & configuration of supported applications
- Performance monitoring of supported applications
- Software patches & upgrades of supported applications
- 24x7x365 maintenance & support of supported applications

Database Management

- Installation and configuration of database
- Database administration
- Software patches and upgrades
- Database monitoring
- 24x7x365 maintenance and support of supported database applications

Web Server Management

- Installation and configuration of http software
- Software patches and upgrades
- Server monitoring

Data Backup & Restoration Management

- Backup administration
- Daily incremental and full weekly backups
- 24x7x365 maintenance and support of backup agent

Monitoring/Reporting

- Reporting with an overview and update on your solution
- Server summary graphs
- Inbound and outbound bandwidth reports that the client can generate based on any specific timeframe (network)
- Disk, CPU, and memory threshold monitoring
- Content checking (server)

Managed Security

- Patch Management
- Continuous Audit
- Advanced Change Control
- PCI DSS Firewall Review
- Web Application Firewall
- Intrusion Detection Service
- Vulnerability Assessment
- Event Management
- Malware Protection
- Data Encryption
- Reporting

Dedicated Server Hosting

Dedicated Server Hosting solutions feature hardware that is housed in Datapipe's secure, geographically diverse, PCI certified facilities. All equipment that stores, processes, or transmits client data resides behind client dedicated firewalls in segmented Virtual Local Area Networks (VLANs), which are managed and secured by Datapipe's certified staff in accordance with various compliance standards and best security practices. Physical solutions can be completely customized in terms of solution architecture, hardware types, number of servers/firewalls, and geographic location of the equipment.

The service offering also includes:

- Equipment maintenance
- Resolution of detected failure within specified guidelines
- Administration of vendor maintenances and patches
- Maintenance of physical security within Datapipe's data centers
- Inventory maintenance of specified hardware

Dedicated Server Hosting services provide clients with Datapipe’s personnel, facilities, and expertise to manage/maintain all equipment, hardware, and firmware on a 24x7x365 basis.

Managed Cloud for AWS

Datapipe is an AWS Premier Consulting Partner and a provider of Managed Cloud for AWS. As an AWS Premier Consulting Partner, Datapipe combines extensive managed services experience with AWS’ elastic infrastructure in order to develop cloud computing solutions for the enterprise.

Datapipe Managed Cloud for AWS includes architecture, design, migration, provisioning support, configuration, storage/backup, security monitoring, and other services that are associated with a managed service environment but not available on the raw AWS infrastructure. Managed Cloud for AWS clients can also continue to utilize Amazon’s web management portal.

Datapipe and AWS services are available to clients, including:

- 24x7x365 Issue Response and Resolution, AWS Cloud provisioning, Managed Scaling, Managed security groups and anti-virus, Advanced Monitoring, and Governance
- Access to Datapipe’s ITIL-based service management portal, Datapipe One
- Database, OS, Network, and Storage Management services
- Provisioning support, cloud lifecycle management and orchestration, and best practice design and architecture planning
- Service Level Agreement (SLA) backed event response times and Enhanced availability SLA (greater than 99.95%) available upon Datapipe approval of a High Availability Design

PCI Stratosphere Virtualization Platform (PCI vStrat)

Datapipe’s PCI DSS audited and certified Stratosphere® Virtualization Platform (PCI vStrat) provides private cloud-based solutions featuring the degree of control required of compliance solutions. Stratosphere® consolidates server hardware by running software applications on Virtual Machines (VMs) deployed across a highly scalable infrastructure.

The solution includes the platform itself; the management network and ESX hosts, as well as Datapipe 24x7x365 support. The platform is exclusive to VMs that receive Datapipe’s full PCI package, which conforms to the recommendations in the PCI Security Standards Council (SSC) Virtualization Guidelines to not implement Mixed-Mode for shared hypervisors or physical hosts.

PCI vStrat Features

- Hardware or virtual firewall available
- A combined hardware, software, and Storage Area Network (SAN) solution
- Architected to meet the HIPAA and PCI compliance requirements
- Fixed Cost Model
- Firewall
- VPN Access Available including 2-factor VPN
- 24x7x365 immediate live support
- Enterprise Service Level Agreement

- Disaster Recovery and High Availability environments available

Hybrid

Hybrid deployments are offered to clients, which allow them to combine physical and cloud features into a solution that meets their business and budgetary needs. In a hybrid deployment, clients receive the security benefits of a private cloud with the commercial benefits of a public cloud. As with the PCI-Certified Stratosphere® Virtualization Platform deployment model, sensitivity levels are not mixed on the same hypervisor.

Datapipe’s Hybrid Cloud Connect allows clients to connect their cloud to their infrastructure in any of Datapipe’s global data center facilities. Clients can take full advantage of the elasticity and scalability of the cloud when they link their physical environments. A Virtual Routing & Forwarding (VRF) solution can connect Datapipe private cloud, public cloud, and dedicated servers to create a true integrated platform capable of meeting various computing needs. The Cisco-based network platform is designed for the enterprise to create a secure, low latency internal network that links dedicated infrastructure to cloud resources.

HIPAA Compliant Hosting

Datapipe’s Comprehensive Security Compliance and HIPAA Solutions provide the network infrastructure, physical security, and the technical controls to safeguard client’s data within segregated environments. Datapipe offers the variety of deployment models noted above: managed physical, cloud, and hybrid environments. All of these deployment models are hosted within Datapipe’s secure, geographically diverse facilities that are HIPAA compliant, and subject to annual System and Organization Controls (SOC) examinations. Solutions can be completely customized in terms of solution architecture, hardware, number of servers/firewalls, and geographic location. For all deployment models, Datapipe solutions are supported by full-time on-site engineers and physically secured 24x7x365 by security personnel, badge/photo ID access screening, biometric access screening, motion sensors, and security breach alarms.

Datapipe leverages the Payment Card Industry Data Security Standard (PCI DSS) as a prescriptive security baseline for implementing controls for its hosted HIPAA solutions. This standard outlines a comprehensive framework of detailed security controls, technologies, and implementation standards for securing credit card data.

As a managed IT service provider that does business with healthcare organizations, Datapipe maintains the infrastructure of client systems that handle electronic protected health information (ePHI). While Datapipe employees do not manage or operate healthcare applications directly, and therefore do not have a business need to access or alter such ePHI, its employees do have a need to administratively manage such systems.

Therefore, as a maintainer of ePHI, Datapipe will enter into a Business Associate Agreement (BAA) with a covered entity (CE), provided that the compliance package is elected in its entirety. This package has been specifically designed as a result of Datapipe’s internal risk assessment to help safeguard client ePHI, reduce risk of disclosure, and comply with the regulations as mandated by the Office of Civil Rights.

Datapipe meets all HIPAA Administrative Safeguards (§164.308) and Physical Safeguards (§164.310) with respect to its policies, procedures, processes, employees, and data centers worldwide (as applicable to Business Associates and Datapipe’s services). Additionally, election of Datapipe’s Compliance

Package – HIPAA Edition aids covered entities in addressing Technical Safeguards (§164.312) as required by HIPAA regulations.

PCI Compliant Hosting

Datapipe's Comprehensive Security Compliance and PCI Certified Solutions provide the network infrastructure, physical security, and the technical controls to safeguard clients' cardholder data within their segregated environments. These solutions are built upon the compliance standards defined by PCI DSS.

In compliance with these requirements, Datapipe provides a complete PCI security solution to help clients achieve and maintain compliance. Each of the following services have been configured to meet or exceed an associated PCI DSS requirement, and to ensure the proper monitoring and maintenance of client Cardholder Data Environments (CDE):

- Dedicated Managed Firewall
- PCI Firewall Review
- Web Application Firewall
- Malware/Antivirus Protection
- Vulnerability Assessment and Notification
- Event Management
- Intrusion Detection Services
- Two-Factor VPN Authentication
- Patch Management
- Secure Server Configuration Monitoring and Management
- File Integrity Monitoring
- Transparent Database Encryption (TDE)
- File Encryption

Additionally, Datapipe is a Level 1 PCI Certified Service Provider. As required, Datapipe undergoes regular third-party QSA audits to ensure internal compliance. Datapipe's status as a PCI certified service provider can be referenced in Visa's global registry: http://www.visa.com/splisting. More details on Datapipe's annual PCI DSS audit can be found in its Report on Compliance.

Data Center Services

Datapipe's data center services provide customers with the physical security controls, power management and facility space needed for the continued functionality of critical hardware. The sites offer reliability, redundancy, security, customization, power, and cooling availability to meet the requirements of their customers. The Datapipe colocation services may include, but are not limited to, the following:

- Expert support engineers onsite 24 hours per day
- Security personnel patrolling at all times
- Code of conduct reviews for all facility staff
- Badge / photo identification (ID) access screening and biometric access screening for added levels of security

- Motion sensors and security breach alarms protecting restricted areas
- Strict access policies, requiring all visitors to pass through multiple levels of security and be escorted at all times
- Operational surveillance camera system with archived footage available for review
- Power systems with built-in redundancy
- Uninterruptible power supply (UPS) and / or diesel rotary uninterruptible power supply (DRUPS) systems with N+1 redundancy levels or greater in the event of a local utility failure
- Power distribution units (PDU) to distribute electric power to the colocation customers
- Diesel generators for back-up power
- Heat, ventilation, and air conditioning (HVAC) systems to cool the most demanding high-power deployments
- Very early smoke detection apparatus (VESDA) fire detection systems
- Dry pipe fire suppression systems
- 24 hour per day environmental control monitoring and alerts

Within the data center facilities, the following options are available to customers to meet specific requirements for physical security and power usage:

- Suites: hard-walled rooms for colocation customers requiring more data center space and dedicated security features.
- Cages: an enclosure that subdivides colocation space within a data center using mesh walls, a door, security panels, and access badge readers (or keys, depending on location).
- Cabinets: a closed structure that houses servers typically made of metal with rails, grounding studs, interior shelving, and wire racks.

Network Availability

Datapipe provides colocation customers with direct connectivity to the Datapipe network, backed by SLAs that guarantee a round-trip transmission speed of, on average, 90 milliseconds or less between Datapipe-designated inter-regional transit backbone network routers in North America, and round-trip transmission of 120 milliseconds or less between a Datapipe-designated hub router in the New York metropolitan area and a Datapipe-designated hub router in the London metropolitan area.

The New Jersey One and New Jersey Two facilities provide the following networking capabilities:

- Connections to all geographically available Tier 1 providers (Carrier-neutral facility)
- Peering connections with over 200+ providers at major telecommunication hotels
- Dedicated dark fiber ring with diverse paths and full redundancy
- Additional bandwidth wave from Ashburn, Virginia
- Encrypted multi-protocol label switching (MPLS) connectivity to other Datapipe data centers
- Direct fiber connectivity to primary New York City point-of-presence (POP)
- Full support for fiber channel, Synchronous Optical Networking (SONET), and Ethernet hand-offs

- Datapipe also makes available its full suite of managed services to colocation customers on an as needed basis. Datapipe refers to this offering as "Molo", or managed colocation

The Silicon Valley One facility provides the following networking capabilities:

- Meets Bellcore network equipment building systems requirements
- Redundant fiber sources, aggregate switches, and core routers
- Connections to all geographically available Tier 1 providers via redundant minimum point of entry (MPOE) fiber vaults
- Peering connections with over 200+ providers at major telecommunication hotels
- Encrypted MPLS connectivity to other Datapipe data centers

Customer requests for services are initiated and authorized by user entities by directly contacting the customer support department. Customer requests are recorded and tracked within an internal ticketing system through resolution. The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established service level agreements.

THE BOUNDARIES OF THE SYSTEM COVERED BY THE DESCRIPTION

This report includes the Datapipe Managed Cloud and Hosting Services solutions. Any other Datapipe services are not included within the scope of this report. The accompanying description includes only policies, procedures, and control activities at Datapipe and does not include policies, procedures, and control activities at any subservice organizations.

The boundaries of the system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

The Company uses third-party subservice organizations for data center colocation services. Section 4 of this report and the description of the system only cover the Trust Services Principles and Criteria and related controls of the Company and exclude the related controls of the subservice organizations. Although the subservice organizations have been carved out for the purposes of this report, certain controls are expected to be in place at the subservice organizations related to physical security and environmental protection.

MONITORING OF SUBSERVICE ORGANIZATIONS

The third-party data centers utilized by Datapipe provide physical and environmental security controls to prevent physical attacks and/or loss of availability and mitigate the risk of fires, power loss, climate, and temperature variabilities. Datapipe monitors these controls by obtaining and reviewing audit or attestation reports of the third-party data centers on an annual basis.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

MANAGED CLOUD AND HOSTING SERVICES

- Management Network - Secure Access Network for Transparent Administration (SANTA)
  - A secure isolated network used by authorized employees to remotely manage Client resources.
  - Accessible only to authorized employees by leveraging a SSL Two Factor VPN.
  - PCI compliant environment leveraging security best practices and Datapipe’s enterprise security controls.
- Configuration Management Database (CMDB) - Datapipe One (DP1)
  - Includes ticketing, change management, incident management, and problem management.
- AWS Management – Cloud Management System (CMS) and Datapipe Access and Audit Control for the Cloud (DAAC)
  - Role-based access control platform for Datapipe support personnel management of AWS resources.
  - Accountability achieved with all system access and activities tied to Datapipe support user’s unique account.
  - Leverages two-factor authentication for Datapipe employees via Single Sign On.
  - Employees’ keys are stored in Secret Server and never exposed to the employees themselves.
  - Client administrative API keys are not required for Datapipe AWS console administration
- PCI Community Cloud Platform (PCI vStrat)
  - PCI compliant platform leveraging security best practices and Datapipe’s enterprise security controls.
  - Community based platform ensuring all guests perform payment card workloads.
  - A non-mixed mode policy ensures all guests are at the same security level.
  - Tenants on the PCI vStrat platform are logically isolated from all other tenants.
- Password Management / Password Vault
  - A role based password vaulting system used by Datapipe employees to securely access internal and external credentials.
  - Password check-in/check-out functionality ensure a credential is rotated after each use.
  - Leverages strong-cryptography and hardware security modules (HSM)

MONITORING

Datapipe’s support engineers monitor internal infrastructure and client solutions 24x7x365. Monitoring Services continuously verify the viability of critical resources, processes, and services that are essential to client solutions. Dashboards represent a comprehensive performance/health view of a device infrastructure, application environment, and/or service. Operational dashboards utilize multi-tenancy and user policies to control access and device visibility. Monitoring services can capture performance statistics and send alerts when availability thresholds have been breached for the following system parameters: Protocols (ICMP, HTTP, FTP, SMTP, etc.), CPU utilization, memory utilization, disk storage capacity, and running processes/applications.

Datapipe’s monitoring infrastructure includes:

- Platform
  - Hardware and software solutions that have been engineered and designed to meet the demands of Datapipe’s Management Appliances
  - Monitoring has online backup solution for 24x7x365 operations with data recovery
- Redundancy and High Availability
  - Automated database failover and clustering with disaster recovery system
- Data Management
  - Performance tuned data repository
  - Data normalization for long-term data analysis
  - Systems have customizable threshold alerting and reporting
- Security
  - Encryption connection between database and remote collectors
  - Customized user permission keys and controlled user access
  - Audit logging of user activity

Backups

Datapipe manages and provides a variety of host-based backup storage options to mitigate the risk of losing vital data and to meet specific internal and client system needs. Storage architects consult with system owners and clients to determine the best backup technique based on data types, storage system, and Recovery Point Objective/Recovery Time Objective (RPO/RTO) requirements. Datapipe’s enterprise backup solution is powered by Veritas’ NetBackup software suite and EMC’s Data Domain storage.

Backups are maintained on a variety of systems based on type, retention time, file size, backup time, and recovery time requirements. The monitoring team receives automatic notification of backup status, and takes steps to ensure that issues are resolved in a timely manner. In the event of data loss, or upon system owner/client request, Datapipe can restore the environment from the available backup.

Summary of capabilities:

- Design and implementation support
- Managed storage solution in multi-platform environments
- SAN/NAS capable snapshot backups
- Monitored backups to ensure job completion
- Quick restore of large datasets via snapshots
- Dedicated backup options available
- Fully customizable backup scheduling
- Stored in PCI Level 1 compliant Datapipe Data centers
- Dedicated backup network port for each server
- Restore requests via "Datapipe One - Advanced Client Portal"
- Encrypted MPLS moves data for off-site backups
- Backup reporting available with customized or daily reporting on backups available

- As an AWS Premier Consulting Partner, Datapipe can design and manage AWS backups with options including utilizing S3 and Glacier depending on client use cases

Data Center Services

Specifics for the data center facilities that are owned by Datapipe include, but are not limited to, the following:

New Jersey One and New Jersey Two (Somerset, New Jersey)

HVAC

Server rooms are maintained at a controlled temperature of 72 degrees Fahrenheit, plus or minus 7.5 degrees, and relative humidity is maintained at 45%, plus or minus 10%, as measured at the intake of Datapipe's computer room air conditioning (CRAC) units. The environment is maintained by utilizing the following:

- CRAC units with N+2 implementation
- Hot / cold aisles with hot aisle containment
- Raised floor cold plenum supply, ceiling warm return plenum to provide uniform cooling distribution

New Jersey One’s HVAC system consists of two separate glycol loops which are fed by dry coolers and pumps. There are two glycol pumps per system, controlled by variable frequency drives (VFD) with the capability to transfer from one pump to another in case the lead pump fails. The dry coolers are controlled by VFDs to optimize energy and fan speed control.

All CRAC units, dry coolers, and pumps are electrically fed by two separate panels to ensure that 50% of the cooling capabilities can be maintained if one panel fails. All HVAC equipment is backed up via generators. HVAC equipment is monitored from the building management system (BMS), and all alarms are acted on by the facilities team.

Humidification is controlled internally by the CRACs, which are equipped with an ultrasonic humidification system. The humidity is monitored via the CRAC units and the BMS.

The New Jersey Two facility utilizes two different HVAC systems. The system used in the managed services data hall utilizes a glycol system for the CRAC units. This is a one to one system and each CRAC unit has an associated dry cooler located on the roof. Each dry cooler has a redundant pump attached to it. The CRAC and dry cooler units are dual fed electrically, from two separate sources via a transfer switch.

Humidification is monitored by Stultz humidifiers. There is a control panel in each colocation room with humidity sensors in each. There is a master deionization (DI) plant in the engineering office which supplies deionized water out to the humidifiers via stainless steel piping.

Colocation areas utilize direct expansion (DX) units, which are Freon units with condensers dedicated for each unit. Each unit is dual fed electrically from two separate sources via a transfer switch. All HVAC equipment is backed up via generators. HVAC equipment is monitored from the BMS, and all alarms are acted on by the facilities team.

Fire and Water Damage Detection and Mitigation

New Jersey One and New Jersey Two utilize dual inter-locking pre-action systems, requiring two smoke heads to be triggered before the lines fill with water, then a sprinkler head must be activated by heat before water will be dispersed through the affected zone. There are smoke heads and sprinklers in the drop ceiling and below the raised floors. This system also utilizes a VESDA, a system designed for early detection of smoke and / or small particles. Carbon fire extinguishers are located in all server rooms.

All New Jersey One and New Jersey Two data center halls are capable of leak detection. A BMS alert is sent out if a leak is detected, notifying staff of the specific location and footage of the leak. All data center halls are on raised flooring to keep the customer equipment above the sub floor, and away from any potential water. Floor tiles and / or leak detection maps indicate cable length and where the leak is detected. Devices that regularly carry moisture such as CRAC units are surrounded by leak detection.

Power Conditioning

The New Jersey One facility is capable of providing, at minimum, 145 watts per square foot, and has been designed to provide redundant and reliable power by utilizing the following:

- Redundant 2,500 kilovolt amperes (kVA) transformers
- N+N backup generator infrastructure with 5,000 gallons of diesel per generator
- Two contracted fuel suppliers, on call 24 hours per day
- Fully redundant UPS systems with N+N implementation

New Jersey One is powered by two independent 3,000 amp services which provide power to multiple UPS systems and mechanical panels. All critical loads are protected and backed up by multiple UPS systems which feed out to the PDUs. The PDUs then supply power to the customer racks. Datapipe also offers an A+B redundant feed to each customer rack.

The entire site is backed up by two 2 megawatt (MW) generators and one 750 kilowatt (kW) generator. Each 2MW generator has a 5,000-gallon belly tank for fuel and the 750kW generator has a 3,500-gallon belly tank. Each generator has a built-in Algae X fuel filtration system to ensure clean fuel. The generators are run and tested weekly.

In the event of a power outage, the UPS systems can support typical loads for fifteen minutes while the generators come online. The generators will automatically pick up the load within twelve seconds after utility loss.

The New Jersey Two facility is capable of providing, at minimum, 200 watts per square foot, and has been designed to provide redundant and reliable power by utilizing:

- Separate, redundant 13.2 kilovolt (kV) data center entrance feeds with N+N design
- N+N backup generator infrastructure with 40,000 gallons of diesel onsite
- Two contracted fuel suppliers, on call 24 hours per day
- Dual A+B circuit feeds to each rack, with 30 ampere (AMP) / 208 volts alternating current (AC) N+N implementation
- Fully redundant UPS systems with N+N implementation

The New Jersey Two electrical infrastructure consists of a full system plus system (N+N) power distribution system that provides two sources of electrical power for all critical and essential components. This serves to greatly increase the likelihood of continuous power delivery to the installed IT equipment in any part of the facility. This is accomplished through groups of UPS systems, two utility service entrances with separate distribution switchboards and two engine-generator plants, each of which is backed up by two 1,050kW generators.

The IT equipment is supported through six separate pairs of UPS systems; these pairs support dedicated loads. Power can be shared between the two units of each pair or supported entirely from one UPS system when one system must be shut down for maintenance or repairs. Downstream from each pair of UPS systems is a pair of static transfer switches that will serve as a point of defense against dropping part of the load in the event of an internal UPS system failure.

The key circuit breakers in the distribution systems, including the generator breakers, UPS input breakers and UPS maintenance bypass breakers, are monitored by the BMS, and their status is shown on the active one-line diagram. Load data shall be shown on the active one-line diagram from data captured at the various components of the power system that have onboard metering.

The New Jersey One and New Jersey Two data centers are powered by 100% renewable wind energy.

Security

Facility security is maintained by utilizing three-factor authentication for the entrances, multiple mantraps with reinforced walls, 24 hour per day facility monitoring, and 24 hour per day security staff. The facilities are also under 24 hour internal and external video surveillance, and video is retained for a minimum of 90 days. Visitors are escorted by authorized personnel at all times. The colocation cages in New Jersey Two are outfitted with card readers to restrict access to customers with colocation access rights granted by the designated customer super user.

Silicon Valley One (San Jose, California)

HVAC

Server rooms are maintained at a controlled temperature of 72 degrees Fahrenheit, plus or minus 7.5 degrees, and relative humidity is maintained at 45%, plus or minus 10%, as measured at the intake of Datapipe's CRAC units. The environment is maintained by utilizing the following:

- CRAC units with N+2 implementation
- Hot / cold aisles with hot aisle containment
- Raised floor cold plenum supply, ceiling warm return plenum to provide uniform cooling distribution
- End-to-End colocation cooling is provided via N+2 for redundancy and reliability. The facility features 18” raised floor environment with hot and cool aisle configurations designed to cool 9’ rack / cabinet densities that may reach 200 watts (W) per square foot in areas. Cooling is provided by multi-redundant CRAC units.

Fire and Water Damage Detection and Mitigation

Silicon Valley One utilizes a single interlock pre-action dry pipe system, requiring two smoke heads to be triggered before the lines fill with water, then a sprinkler head must be activated by heat before water will be dispersed through the affected zone. There are smoke heads and sprinklers in the drop ceiling and below the raised floor. This system also utilizes a VESDA, a system designed for early detection of smoke and / or small particles. Edwards System Technology (EST) fire panels monitor smoke detectors, water flow, VESDA, and TraceTek, printing out alarms to the security room printer and broadcasting alarms to engineering personnel's smartphones. Carbon fire extinguishers are located in all server rooms.

Silicon Valley One utilizes the TraceTek water detection system, which uses an under-floor cabling system to detect and indicate leaks in a linear footage manner. These are placed on the perimeter of each colocation to ensure any icing up of evaporator coils on the CRAC units is captured. Additionally, each CRAC unit also has built-in leak detection. A BMS alert is sent out if a leak is detected, notifying staff of the specific location and footage of the leak.

Power Conditioning

The Silicon Valley One facility has been designed to provide redundant and reliable power by utilizing the following:

- Feeds from multiple power grids
- UPS system with N+N architecture
- Five DRUPS systems rated at 1.8MW with N+N architecture
- A single 1.5MW DRUPS system
- Twin 10,000-gallon tank diesel fuel farm shared amongst the six DRUPS systems
- Contracted fuel suppliers, on call 24 hours per day

The Silicon Valley One electrical infrastructure is built in an N+N architecture, designed to indefinitely generate power on-site in the event of utility power loss. Datapipe also has a contract in place with the utility provider for constant provision of 100% facility load. The facility is single fed from two different utility Company circuits.

Silicon Valley One utilizes two types of UPS, including DRUPS and UPS systems. The DRUPS systems are comprised of a spinning power generator and flywheel, powered in a normal state by standard grid power. This power generator supplies clean power to critical systems. In the event of grid loss, stored generator energy continues through inertial spin via the flywheel. During this time, attached engines are started and a clutch engaged, resulting in continual spin of the power generator and flywheel. Redundant on-site fuel storage systems and refuel-on-the-fly commitments allow indefinite self-power generation and delivery in the event of long-term power grid loss. The fuel control systems monitor leaks in double-contained piping and diesel tanks, and monitors tank levels. This system provides the ability to manually transfer fuel from tank-to-tank in order to keep levels even. Service notifications to engineering personnel are displayed on the fuel panel display, and alarms echo to the fire panel / printer in the security room, which is monitored 24 hours per day.

The 1MW UPS system is installed with battery backup and a generator backup. The UPS system provides backup power to the colocation PDUs. Every colocation room features dual fed static switch / PDUs and remote power panels (RPP).

A high resistance ground system is utilized to prevent a short circuit from affecting critical loads. The system is designed to absorb the energy from a short circuit and only allow minimal current to pass to ground, not substantial enough to trip a breaker. An alarm signal is generated on the switchgear as well as the BMS, enabling personnel to trace the ground fault and correct the problem.

An advanced facilities control center (FCC) with dynamic re-routing switching architectures allows Datapipe to perform maintenance on any portion of the power architecture while still maintaining N+1 redundancy.

Security

Facility security is maintained by utilizing three-factor authentication for the entrance, 24 hour per day facility monitoring, multiple mantraps with reinforced walls, and 24 hour per day security staff. The facility is also under 24 hour per day internal and external video surveillance, and video is retained for a minimum of 90 days. Visitors are escorted by authorized personnel at all times. The Silicon Valley One data center utilizes card readers for shared cages, to restrict access to customers with colocation access rights granted by the designated customer super user. Individual cages are secured using tumbler locks. The facility exterior’s radius structure meets Level III / explosion resistance security standards.

Kansas City

HVAC

Server rooms are maintained at a controlled temperature of 72 degrees Fahrenheit, plus or minus 7.5 degrees, and relative humidity is maintained at 45%, plus or minus 10%, as measured at the intake of Datapipe's computer room air conditioning (CRAC) units. The environment is maintained by utilizing the following:

- CRAC units with N+2 implementation
- Hot/cold aisles with hot aisle containment
- Raised floor cold plenum supply, ceiling warm return plenum to provide uniform cooling distribution

Fire and Water Damage and Mitigation

Kansas City utilizes a single interlock pre-action dry pipe system, requiring two smoke heads to be triggered before the lines fill with water, then a sprinkler head must be activated by heat before water will be dispersed through the affected zone. There are smoke heads and sprinklers in the drop ceiling and below the raised floors. This system also utilizes a VESDA, a system designed for early detection of smoke and/or small particles. Carbon fire extinguishers are located in all server rooms.

Power Conditioning

The Kansas City facility has been designed to provide redundant and reliable power by utilizing the following:

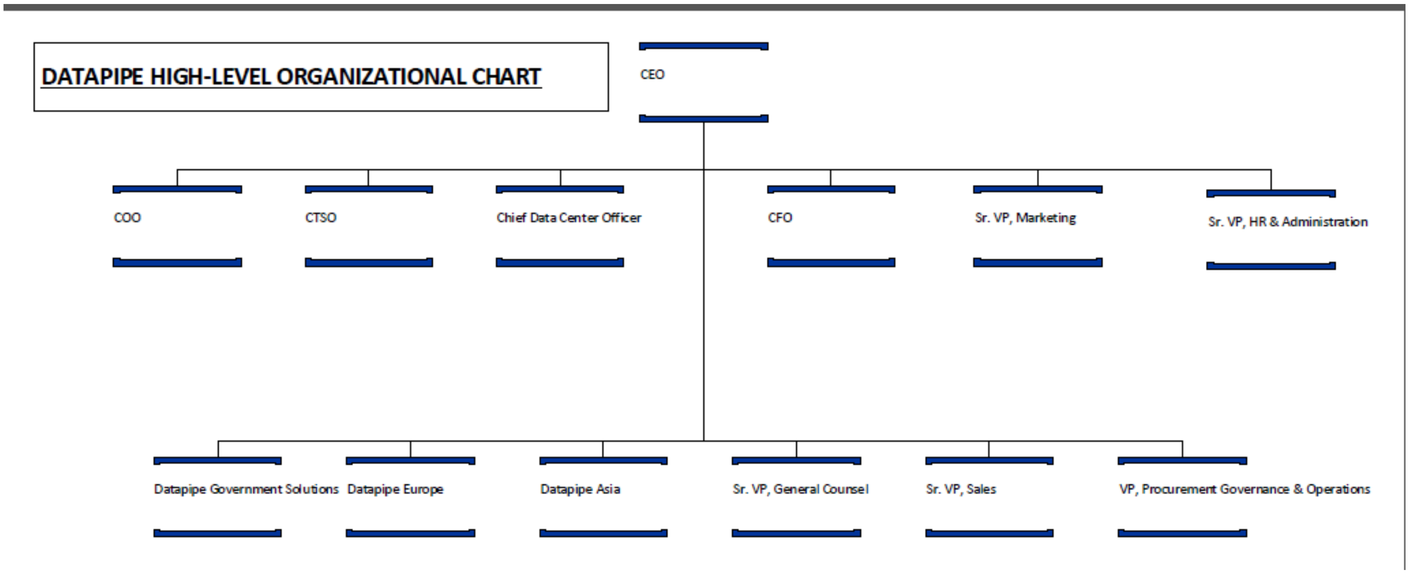
- Feeds from multiple power grids
- UPS system with N+N architecture
- Contracted fuel suppliers, on call 24 hours per day

Security

Facility security is maintained by utilizing three-factor authentication for the entrance, a mantrap to the data center with reinforced walls, 24 hour per day facility monitoring, and 24 hour per day security staff. The facility is also under 24 hour internal and external video surveillance, and video is retained for a minimum of 90 days. Visitors are escorted by authorized personnel at all times.

Functional Areas of Operations

The following organizational structure is in place to support the in-scope data center facilities:


DATAPIPE HIGH-LEVEL ORGANIZATIONAL CHART
CEO
COO
CTSO
Chief Data Center Officer
CFO
Sr. VP, Marketing
Sr. VP, HR & Administration
Datapipe Government Solutions
Datapipe Europe
Datapipe Asia
Sr. VP, General Counsel
Sr. VP, Sales
VP, Procurement Governance & Operations

- Chief executive officer (CEO): responsible for overall Company oversight and leadership, strategic planning and direction, marketing, product, and business development
- Chief technology officer (CTSO): responsible for developing and implementing the technology roadmap for the Company, managing and driving the Company's development program, including Cloud and Operational Support Systems, and working closely with clients and potential clients on complex technological issues and solutions. The CTSO is also responsible for corporate and customer oriented security services development and delivery, physical and logical security, related policies and procedures, security awareness program, and security compliance implementations
- Chief data center officer (CDCO): Responsible for the overall activities of all global data centers, including operations, maintenance, facilities, and uptime
- Chief operations officer (COO): responsible for increasing organizational efficiency through the implementation of controlled processes designed to improve customer support, reporting, and staff alignment
- Senior director of technical operations: responsible for developing and implementing strategies to improve customer support services to customer systems in the data centers
- Director of global response center: responsible for managing the operations of Datapipe's 24 hour per day network to ensure there is no unscheduled downtime
- Data center operations managers: responsible for managing infrastructure capacity planning, establishing operational procedures, developing data center metrics, establishing best practices, analyzing, and escalating site conditions, managing the provisioning of customer infrastructure, and overseeing the data center engineering staff

Datapipe utilizes the specific functional areas of operations within the Managed Services system including:

- System administration – Responsible for functions such as configuration management, patch management, antivirus/anti-malware administration, monitoring services, issue escalation and troubleshooting, and backup procedures.
- Network administration – Responsible for functions such as management of network infrastructure including switches, firewalls, load balancers, routers, and VPN platforms.
- Database administration – Responsible for functions such as database instance management, backup engineering and operations, performance optimization, replication support, database mirroring, and data restoration services.
- Customer Support – Responsible for functions such as dedicated client support, troubleshooting, issue and problem management, escalation, and resolution procedures.

Data Management

Datapipe maintains an in-house development team specialized in the building and customization of monitoring solutions to gather server statistics, logs and to track system, application, and environment status. These custom designed solutions monitor client environments 24 hours per day to maintain the integrity and availability of client systems. Datapipe reviews data collection techniques on a regular basis for improvement and optimization.

An Online Client Portal provides clients the ability to submit support tickets and access various reports that include:

- Statistics on basic capacity utilization and bandwidth
- Real-time system configuration information
- Backup quota status and trending
- Software update management and tracking
- Managed name system services
- User account configuration options
- Invoice history
- A secure file upload location for updates and reports

Custom reports can also be created for clients based upon specific requests.

COMMITMENTS AND SYSTEM REQUIREMENTS

COMMITMENTS

Commitments are declarations made by management to customers regarding the performance of Datapipe, Inc.’s Managed Cloud and Hosting Services. Commitments are communicated in Master Services Agreements. The Company’s commitments include the following:

- Nondisclosure of confidential information.
- Providing logical and physical security.
- Providing 100% up time access to the Datapipe network.

- Providing 100% AC power availability to Datapipe equipment.
- Responding to and resolving incidents.
- Datapipe will use commercially reasonable efforts to maintain acceptable performance of the Services.

SYSTEM REQUIREMENTS

System requirements are specifications regarding how Datapipe, Inc.'s Managed Cloud and Hosting Services should function to meet the Company's commitments to customers. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Risk assessment standards
- Change management controls
- Monitoring controls

AVAILABILITY

The availability principle refers to the accessibility of the system or services as committed by the Company's MSA. The availability of the Managed Cloud and Hosting Services is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient Internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of back-up procedures, the reliability of the back-up process, and the ability to restore backed-up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system elements.

The Company has put controls in place to address the availability risks described above, including the following:

- An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.

- An automated backup system is configured to perform daily differential incremental and weekly full backups of client data, unless the frequency is modified by the client.
- Disk backups of client data are replicated to an offsite data center on a daily basis.
- Backup failures are monitored and email alerts are configured to send to backup administrators. Tickets are created to track and resolve backup issues.
- A documented DR plan is in place.
- A DR test is performed at least annually.
- The Company uses multiple production data centers with significant geographical separation to mitigate the risk of system disruption due to natural disaster or loss of services.
- The Company tests restoration of data at least annually or as part of normal business operations.

In addition, at the data centers owned by Datapipe, the Company has deployed the following controls:

- An environmental monitoring system is in place and configured to monitor and automatically generate an alert to management when predefined environmental thresholds are met.
- The entity has implemented environmental security measures in the data centers that include smoke detectors, fire suppression systems, water detectors installed within the raised floor areas, uninterruptible power supplies, and emergency power supplies.
- Maintenance inspections of fire suppression devices and smoke detectors at Datapipe data centers are performed on an annual basis.
- Maintenance inspections of backup generators, HVAC units, and UPS units are performed on a quarterly basis.

CONFIDENTIALITY

The confidentiality principle addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. Information is confidential if the company that holds or stores information is required to limit its access, use, and retention, and restrict its disclosure to defined parties (including those who may otherwise have authorized access within the boundaries of the system).

The confidential information that the Company maintains includes customer data and other information that customers communicate to the Company during the ordinary course of business.

The Company has designed its controls to address the following confidentiality risks:

- Data is not protected from unauthorized access.
- Confidential information is transmitted to related parties, vendors, or other approved parties contravening confidentiality commitments.
- Related party and vendor personnel are unaware of the entity's confidentiality commitments.
- Confidentiality practices and commitments are changed without the knowledge or consent of internal and external users.

The Company has put controls in place to address the confidentiality risks described above, including the following:

- Administrator access to the network, infrastructure components, operating systems, and databases is restricted to authorized personnel.
- Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access.
- The network is segmented to prevent unauthorized access of customer data.
- Business partners are subject to mutual nondisclosure agreements or other contractual confidentiality provisions.
- Web communication sessions are encrypted via Transport Layer Security (TLS) to protect communications between the system and users connecting to the system from customer networks.
- The Company permits remote access to production systems by authorized employees only with two-factor authentication over encrypted VPN connection.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, MONITORING AND INFORMATION AND COMMUNICATION

CONTROL ENVIRONMENT

The control environment at Datapipe is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment include integrity and ethical values; management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the executive management and operations management.

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 the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Datapipe's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice.

Integrity and ethical behavior are the product of Datapipe's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They 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 Datapipe's values and behavioral standards to personnel through policy statements and codes of conduct and by example. Specific control activities that Datapipe has implemented in this area include the following;

- Organizational policy statements and codes of conduct are documented and communicate entity values and behavioral standards to personnel.
- The employee policy and procedures manual contains organizational policy statements and codes of conduct to which employees are required to adhere.

- Employees are required to sign an acknowledgment form indicating their understanding of their responsibility for adhering to the policies and procedures contained within the manual.
- Employees are required to sign a non-disclosure agreement agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.
- Background checks are performed for employee candidates as a component of the hiring process.

Commitment to Competence

Datapipe management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Datapipe'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 Datapipe has implemented in this area include the following:

- Position requirements are translated into written required skills and knowledge levels based on competence levels for particular jobs.
- Employee performance is evaluated each year through an annual review to help ensure standards of conduct are upheld.
- An external recruiting firm is utilized during the hiring process to qualify the skills of applicants within certain job functions.
- Personnel are provided with orientation, hands-on training and supervision to the extent deemed necessary by management.
- Personnel are encouraged to participate in vendor training and relevant industry certifications.

Executive Management Participation

Datapipe's control consciousness is influenced by their executive management. Attributes include executive management's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management. An executive management is in place to oversee management activities and to monitor management's compliance with the entity's objectives.

Management's Philosophy and Operating Style

Datapipe's management philosophy and operating style is attributed to its commitment to maintaining its system of internal controls. All employees have some role in controlling the organization. Some controls are established at the organizational level, while others are established by the management of the local functional units. Formal policies and procedures have been established to guide personnel on specific information processing and operating functions.

Meetings are regularly held between members of management in finance, operations, and other functional groups to provide and discuss business updates for their respective areas. During these meetings, management discusses various topics including financial results, forecast accuracy, recent or upcoming sales promotions, advertising campaigns, competitor actions, human resources matters, network matters, status of information technology projects, regulatory matters, and various other issues.

Organizational Structure and Assignment of Authority and Responsibility

Datapipe’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Datapipe’s management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Datapipe 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.

Datapipe’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 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 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. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.

Human Resource (HR) Policies and Practices

Datapipe’s HR policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. Specific control activities that Datapipe has implemented in this area include the following:

- Documented HR policies and procedures are maintained to guide HR personnel during the hiring, training, and termination process.
- Pre-hire screening procedures are utilized to include the following:
  - Review of candidate’s resume
  - Interview(s)
  - Skills testing, as applicable
  - Reference checks
  - Background screening
- Performance evaluations are conducted for employees on an annual basis.
- A new hire request form is utilized to help ensure that specific elements of the hiring process are consistently executed.
- A termination ticket is utilized to help ensure that specific elements of the termination process are consistently executed.

RISK ASSESSMENT

Datapipe has implemented a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable infrastructure hosting and physical security services to its customers. These risks address the broad categories of operations, reporting and compliance as well as opportunities for potential fraud within these categories.

This process requires management, under the advice of subject matter experts, to annually identify significant risks inherent in maintaining security and environmental controls for customers and to implement appropriate measures to monitor and manage these risks. Changes to the control environment which could significantly impact the effectiveness of control activities receive the highest priority during such annual reviews. The risk assessment process has identified risks resulting from the nature of the services provided by Datapipe, and management has implemented various measures designed to manage these risks. Risks identified in this process include, but are not limited to, the following:

- Security risks associated with unauthorized access and theft
- Environmental risks associated with power, cooling, leaks, fire, and humidity

These risks are monitored as described in the “Monitoring Activities” section of this report. The risk level assignment is a factor of the following:

- Likelihood of the risk
- Whether or not mitigating controls are in place
- Business impact, if the risk should occur

Risk Factors

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

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
- Environmental risks associated with power, cooling, leaks, fire, and humidity
- Unauthorized access to internal or client data systems and data

Internal Factors

- Security risks associated with unauthorized access and theft
- Significant changes in policies, processes, or personnel
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

A risk assessment tool acts as a guide to determine an appropriate rating for each risk. A risk matrix details these risks, the associated risk level, the control activity to reduce the risk, and the resultant residual risk level. If the residual risk is not accepted, the risk management process continues, and these risks are augmented with additional controls. Senior management signs-off of the completeness and accuracy of the documented risks, ensuring that residual risks are at an acceptable level.

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area.

Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

Selection and Development of Control Activities

Control activities are a part of the process by which Datapipe strives to achieve its business objectives. Datapipe 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.

MONITORING

Monitoring Activities

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as customer complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. In addition, Datapipe utilizes information produced by their information systems to monitor the control environment such as change control documentation, customer support issue tracking and resolution data, and performance and availability reports.

Effectively safeguarding critical systems requires continual monitoring and appropriate controls in order to prevent and / or mitigate any potentially devastating disasters. Through the use of automated monitoring and alerting systems, testing, systems redundancies, and documented procedures, Datapipe is able to react to system and technology failures and minimize adverse impacts to service. In addition, Datapipe management and supervisory personnel have also implemented a suite of monitoring activities such as spot-checks and periodic reviews to ensure that control activities are performed effectively over time. Non-compliance or other problems that are identified through monitoring are escalated and resolved timely.

Datapipe-Owned Facilities

Datapipe monitors the Security Systems 24 hour per day using multiple processes. A BMS is used to monitor all environmental controls. In addition, system support technicians conduct facility rounds each shift and serve as a secondary check on environment control status.

All monitored system conditions will be brought to the appropriate level of attention. Data center environmental alerts are escalated in accordance with the facility emergency action manuals.

Ongoing and Separate Evaluations of 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 ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Datapipe’s monitoring is integral to complete service delivery. Datapipe’s Layer 1 level monitoring watches operating system functions, i.e. processor utilization and free drive space, as well as service availability. Datapipe’s Layer 3 and Layer 4 level monitoring takes it a step further by monitoring content and functionality levels for the client environment. Custom checks are created at these levels to replicate traffic that the client might expect to see in their environment. These custom checks can include synthetic checks that run transaction processing to test the full functionality of a client environment. Datapipe’s awareness of the client environments provides more proactive maintenance, suggesting fixes and implementing changes to client systems to prevent downtime.

Datapipe’s compliance and security department strives to stay ahead of regulatory changes by actively monitoring and reviewing applicable laws, regulations, and industry standards. These reviews allow Datapipe to implement the required controls prior to the date of requirement. A security awareness program is maintained to monitor security issues through subscriptions to services such as: InfoSec News, Security Focus, and CERT. The department communicates security issues affecting their industry to employees and management via the following methods:

- Security communications posted on the Company Intranet site
- Regular e-mail newsletters sent to all employees
- Security posters displayed throughout working areas
- Upon hire and annual employee training

Servers are monitored by Datapipe’s custom built observer application. Alerts are escalated in accordance with the customer's solution escalation action plan (SEAP), which is tailored to each customer’s solution. Responses are also dictated by the facility emergency action manuals and the customer’s SEAP. These responses are tracked via tickets in both cases with unlimited historical tracking.

Policies and procedures exist to support the facilities’ physical security. This includes procedures for enrollment and review. All individuals entering the facility must be authorized to do so, and they are required to submit to the three-factor authentication procedure.

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.

Datapipe’s security and compliance team and operations management perform weekly and monthly reviews of the internal controls by reviewing activities and the associated change controls. These reviews determine whether processes and procedures are being followed as well as providing opportunity for the controls to be reviewed for optimization.

Management performs regular reviews of change control submissions to verify that the initiator is correctly filling out the form, submitting to the change approval board and escalating any emergency changes for the appropriate approvals. Management also reviews changes to verify that the change approval board is following the defined risk mitigation and approval processes.

Datapipe undergoes PCI DSS, SOC, and ISO27001 certification assessments annually by a third-party auditor.

Reporting Deficiencies

Management has developed protocols to ensure findings of internal control deficiencies should be 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. Datapipe's Operations teams review customer complaints and view them as opportunities to improve service delivery. Each complaint is reviewed and addressed for the client and then expanded as appropriate to client environments.

Any violation of Datapipe security policies (including Authorized Use Policies), processes and procedures or to report other security issues impacting Datapipe and/or Datapipe client's systems hosted at Datapipe facilities must be submitted via the security incident reporting form. The information contained in the security incident report is considered confidential and shall be transmitted, stored, and processed in compliance with Datapipe's Confidential Data Policy, and Datapipe's Incident Response Plan.

The following information is included on the security incident reporting form:

- Description of the event in as clear and detailed language as possible, including any supporting documentation and does not include confidential data in any attachments (i.e., card numbers, account numbers, social security numbers, and other types of personal identifiable information and data).
- Incident Reporting Level, which is crucial for determining how rapidly Datapipe's Incident Response Plan must react to protect Datapipe, clients, and confidential data.

Incidents are tracked by the Datapipe Incident Response Plan in a central repository that includes escalation and links to response.

Datapipe-Owned Facilities

Physical Breach

Should there be a serious incident involving a physical breach of security, officers are instructed to contact the local authorities in accordance with the facility post orders. Additionally, officers shall escalate to the following individuals:

- Security site supervisor
- Data center operations manager
- CSO

In turn, these individuals will escalate to the CDCO and CEO as necessary. Additionally, if the incident were to involve a Datapipe employee, HR is to be contacted as well.

Environmental Alerting, Escalation, and Resolution

In the event of an emergency affecting the data centers' electrical, HVAC, or fire detection and suppression systems, data center personnel are expected to make every reasonable effort to contact the data center chief engineer or another member of the data center engineering team before attempting to troubleshoot. The facility emergency action manuals provide data center personnel with the following:

- Detailed steps for troubleshooting and resolution of issues
- Escalation procedures for issues they are unable to resolve
- Emergency contact information for the data center operations manager, data center engineers, vendors, and emergency services

Customer Reporting

All monitored conditions related to system availability and the system health status that are defined in "System Availability Checks and Health Monitoring" of the SLA are reported in the Datapipe customer portal. E-mail notifications may also be sent to colocation customers in the event of the following circumstances:

- An unexpected outage or service interruption impacted their power and / or connectivity
- Datapipe must perform system and / or infrastructure maintenance that may impact their power and / or connectivity
- Changes are made to Datapipe facility rules and regulations

INFORMATION AND COMMUNICATION

Information Systems

The Datapipe management environments are segmented to help ensure clients' compliance requirements and separate service areas for security on dedicated networks. Access to Datapipe's management networks, both internal and external, is restricted using two-factor authentication using Cisco VPN technology.

Datapipe maintains in-house development teams to build and maintain customized security monitoring and configuration tools for front and back-end technologies utilized by Datapipe's clients. Specific technologies Datapipe's development teams are derived to support include, but are not limited to, the following:

Internet Architecture

- Domain name services (DNS) and systems
- Web services including Microsoft IIS and Apache
- Internet Server Application Programming Interfaces (ISAPI) including Active Server Pages (ASP), .NET, Perl and Hypertext Preprocessor (PHP)

Database Services

- Database services including Microsoft SQL Server, Oracle, MySQL and additional open source and third-party databases
- Development suites supporting array, functional, object-oriented, system, logic, and structured programming languages

Datapipe’s experience and versatility allow a broad range of technologies to be supported. Datapipe is capable of supporting Windows, and Linux environments utilizing hardware infrastructure comprised of enterprise vendors including Hewlett Packard, Dell, Cisco, and VMware.

Datapipe has production systems which are used to:

- Maintain customer information, work requests, and work history
- Monitor customer service infrastructure
- Schedule and track maintenance on site infrastructure
- Collect, dispatch, and track customer support requests
- Identify on-call engineering resources for incident response and support escalation
- Track and identify customer port assignments
- Design site infrastructure layout for customer solutions
- Manage site security access control
- Record and monitor closed circuit television (CCTV) 24 hours per day
- Perform backups of production systems as specified by the customer
- Operating system and application patch management

Datapipe-Owned Facilities

The infrastructures are comprised of multiple bandwidth providers with 1 gigabyte (GB) and 20 GB connections to the network. Datapipe runs border gateway protocol (BGP) with providers to ensure service in the event a single provider loses connectivity or experiences issues on their network, as well as optimizing the packet path for customer solutions by determining the least latency path. The network infrastructure is comprised of a border layer, which handles all bandwidth provider connections, and a distribution layer, which handles the route distribution to the colocation layer, terminating on the collocated equipment. Datapipe can offer hot standby router protocol (HSRP) for redundant uplinks to two different switches, BGP full routing tables with proper customer provided advertisement, and autonomous system numbers (ASN). Connectivity to a redundant pair of switches is available, providing customers the option of single or redundant handoffs to their solution.

The following software packages are utilized to maintain records for environmental systems, as well as manage physical access controls:

- ViconNet: used to view, playback and record digital video surveillance for at least 90 days
- WinDSX SQL: used by card readers to verify user access levels, generate history reports, lock and unlock doors, and generate alarms
- IrisAccess: used to store and validate iris biometric data
- SharePoint: used as a collaboration platform and document repository to store maintenance records, commissioning reports, service contracts, etc.
- Custom BMS: used as a building management system to report on the overall health of all monitored infrastructure equipment
- Datapipe One: used to validate colocation access permissions for tours, temporary, and permanent physical access, as well as document, record, and escalate environmental system events

Communication Systems

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 the Company.

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

TRUST SERVICES PRINCIPLES, CRITERIA, AND RELATED CONTROLS

The Trust Services Principles that are in scope for purposes of this report are as follows:

- *Security*: The system is protected against unauthorized access (both physical and logical).
- *Availability*: The system is available for operation and use as committed or agreed.
- *Confidentiality*: Information designated as confidential is protected as committed or agreed.

Many of the criteria used to evaluate a system are shared amongst all of the principles; for example, the criteria related to risk management apply to the security, availability, and confidentiality principles. As a result, the criteria for the security, availability and confidentiality principles are organized into (a) the criteria that are applicable to all three principles (common criteria) and (b) criteria applicable only to a single principle. The common criteria constitute the complete set of criteria for the security principle. For the principles of availability and confidentiality, a complete set of criteria is comprised of all of the common criteria and all of the criteria applicable to the principles being reported on.

The common criteria are organized into seven categories:

CC1.0 *Organization and management:* The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

CC2.0 *Communications:* The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

CC3.0 *Risk management and design and implementation of controls:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

CC4.0 *Monitoring of controls:* The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

CC5.0 *Logical and physical access controls:* The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principles addressed in the engagement.

CC6.0 *System operations:* The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objectives of the principles addressed in the engagement.

CC7.0 *Change management:* The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principles addressed in the engagement.

This report is focused solely on the Security, Availability and Confidentiality principles and does not include the Processing Integrity and Privacy principles.

The Company's applicable controls supporting the Security, Availability and Confidentiality principles and related criteria are included in Section 4 of this report. Although the applicable criteria and related controls are included in Section 4, they are, nevertheless, an integral part of the organization's description of its System.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

The description does not extend to the services provided by the subservice organizations that provide colocation services for IT infrastructure. Components of certain Trust Services criteria are intended to be met by controls at the subservice organizations. The table below includes each of the applicable trust services criteria that are intended to be met by controls at the subservice organizations, alone or in combination with controls at the service organization and the types of controls expected to be implemented at the carved-out subservice organizations:

Criteria	Types of controls expected to be implemented at the carved-out subservice organizations
CC5.5	Data center access is restricted to authorized personnel through the use of a card key reader. Data centers are monitored by closed circuit cameras. Data centers are monitored 24x7 by security personnel.
A1.2 CC6.1	Data centers have installed fire suppression and detection, and environmental monitoring systems. Data centers are protected against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). Environmental protections at data centers are subject to regular maintenance.

COMPLEMENTARY USER ENTITY CONTROLS

Datapipe’s Managed Cloud and Hosting Services were designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to Datapipe’s managed cloud and hosting services to be solely achieved by Datapipe’s control activities. Accordingly, user entities, in conjunction with the Managed Cloud and Hosting Services, should establish their own internal controls or procedures to complement those of Datapipe.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

System Backups

- User entities are responsible for notifying Datapipe of backup, retention, and disposal requirements that are different than the default parameters.
- User entities are responsible for developing their own disaster recovery and business continuity plans.

Network Services and Monitoring

- User entities are responsible for timely notification of any known or suspected incidents affecting services provided by Datapipe.
- User entities are responsible for creating and communicating specific escalation procedures for problems to their network services and hosts.
- User entities are responsible for notifying Datapipe of required changes to their escalation procedures.
- User entities are responsible for responding to known or suspected incidents reported by Datapipe.
- User entities are responsible for monitoring adherence to service level agreements maintained with Datapipe.

Logical Security

- User entities are responsible for establishing and adhering to security procedures to prevent the unauthorized or unintentional use of information systems and infrastructure.
- User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with Datapipe’s systems.
- User entities are responsible for notifying Datapipe of any terminations involving personnel with access to Datapipe’ systems.
- User entities are responsible for implementing username and password security practices for their applications.
- User entities are responsible for the security of all custom and/or unsupported applications.
- User entities are responsible for application and network penetration testing of their individual environments.
- User entities are responsible for adhering to Datapipe security polices in connection with elected security services.

- User entities are responsible for the security impact for any changes made by its personnel (i.e. system configuration and AWS security group management)

Customer Provisioning

- User entities are responsible for completing scoping questionnaires accurately and completely.
- User entities are responsible for notifying Datapipe of required changes to their solutions in a timely manner.
- User entities are responsible for responding to Datapipe inquiries or notifications regarding their solution in a timely manner.
- User entities are responsible for setting up authorized contacts within the client portal.

Compliance

- User entities are responsible for performing a risk assessment and determining appropriate security controls requirements and implementing such security controls or electing optional Datapipe security services.
- User entities are responsible for identifying to Datapipe any compliance or regulatory mandates and where appropriate, executing corresponding agreements.
- User entities are responsible for the overall compliance of their individual environments.

Customer Service

- User entities are responsible for reviewing proposed solutions and acknowledging the successful completion of issues reported to Datapipe customer service.
- User entities are responsible for reviewing and requesting changes to service level agreements maintained.
- User entities are responsible for providing a list of authorized personnel to Datapipe and for making additions, changes, or deletions.

New Jersey One

- User entities are responsible for ensuring their cabinets and / or cages are locked and their equipment is secured prior to leaving the premises.
- User entities are responsible for informing their vendors of Datapipe’s policies and procedures regarding conduct in the shared colocation facilities.
- User entities are responsible for ensuring their guests and / or visitors are escorted throughout the shared colocation facilities.
- User entities are responsible for providing Datapipe the listing of individuals authorized to access the colocation facilities, and for notifying Datapipe if an individual should be removed from the access list in a timely manner.

Silicon Valley One

- User entities are responsible for ensuring their cabinets and / or cages are locked and their equipment is secured prior to leaving the premises.
- User entities are responsible for maintaining control of their locks and keys for their individual cages.
- User entities are responsible for informing their vendors of Datapipe’s policies and procedures regarding conduct in the shared colocation facilities.

- User entities are responsible for ensuring their guests and / or visitors are escorted throughout the shared colocation facilities.
- User entities are responsible for providing Datapipe the listing of individuals authorized to access the colocation facilities, and for notifying Datapipe if an individual should be removed from the access list in a timely manner.

London One

- User entities are responsible for ensuring their cabinets and / or cages are locked and their equipment is secured prior to leaving the premises.
- User entities are responsible for informing their vendors of Datapipe's policies and procedures regarding conduct in the shared colocation suites.
- User entities are responsible for informing their vendors of Global Switch's policies and procedures regarding conduct in the data center facility.
- User entities are responsible for ensuring their guests and/or visitors are escorted throughout the shared colocation facilities.
- User entities are responsible for providing Datapipe the listing of individuals authorized to access the colocation facilities, and for notifying Datapipe if an individual should be removed from the access list in a timely manner.

CHANGES TO THE SYSTEM

During the examination period, the Company underwent the following changes:

- The San Francisco, California data center location was closed, and all infrastructure was moved to the San Jose, California data center location.
- Datapipe, Inc. was formally acquired by Rackspace, Inc. as of November 16, 2017.

REPORT USE

The description does not omit or distort information relevant to the Managed Cloud and Hosting Services while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

SECTION 4

TRUST SERVICES SECURITY, AVAILABILITY AND CONFIDENTIALITY PRINCIPLES, CRITERIA, RELATED CONTROLS AND TESTS OF CONTROLS

CONTROL ENVIRONMENT ELEMENTS

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, the Code of Conduct, Policies and Procedures and Human Resources.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Datapipe’s organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

DESCRIPTION OF TESTS PERFORMED BY COALFIRE CONTROLS, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability and confidentiality principles and criteria were achieved throughout the period April 1, 2017 to March 31, 2018. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Datapipe’s Managed Cloud and Hosting Services and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listing within management’s description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

COMMON TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY

CC1.0 Criteria Related to Organization and Management

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to the in-scope TSPs.	The Company has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the organization chart to determine that it defined the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
CC1.2 Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to the in-scope TSPs.	The Company has appointed a Chief Technical & Security Officer (CTSO) to be responsible for the development and maintenance of the Company's security, availability, and confidentiality policies and perform routine updates as technology, industry, regulatory, and business requirements change.	Inspected the security policies to determine that the Company had appointed the CTSO to be responsible for the development and maintenance of the Company's security, availability, and confidentiality policies and perform routine updates as technology, industry, regulatory, and business requirements change.	No exceptions noted.

CC1.0 Criteria Related to Organization and Management

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting the in-scope TSPs and provides resources necessary for personnel to fulfill their responsibilities.	The Company has written job descriptions specifying the responsibilities along with academic and professional requirements for employees.	Inspected job descriptions for a sample of employees to determine that roles and responsibilities were defined for each employee sampled.	No exceptions noted.
	The Company requires all personnel to undergo security awareness training as part of the on-boarding process and annually thereafter.	Inspected training documentation to determine that security awareness training included development in system security concepts and issues.	No exceptions noted.
		Inspected training completion evidence for a sample of new hires to determine that security awareness training was completed as part of the on-boarding process for each new hire sampled.	No exceptions noted.
		Inspected training completion evidence for a sample of employees to determine that security awareness training was completed for each employee on an annual basis.	No exceptions noted.
	As part of the security awareness training program, the Company requires all employees to affirm that they have received and understand the Company's security policies upon hire and annually thereafter.	Inspected security policy acknowledgements for a sample of new hires to determine that employees were required to acknowledge that they had read and agreed to the Company's security policies upon hire.	No exceptions noted.

CC1.0 Criteria Related to Organization and Management			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
		Inspected security policy acknowledgements for a sample of employees to determine that employees were required to acknowledge that they had read and agreed to the Company's security policies on an annual basis.	No exceptions noted.
	Managers are required to complete performance appraisals for direct reports at least annually.	Inspected performance appraisals for a sample of employees to determine that performance appraisals were completed by management on at least an annual basis for each employee sampled.	No exceptions noted.
CC1.4 The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to the in-scope TSPs.	New personnel offered employment are subject to background checks. In certain jurisdictions where the Company operates, background checks are either not legal or not customary. In these jurisdictions, the Company performs other background screening procedures for new personnel, such as reference checks.	Inspected a background check confirmation or reference check documentation for a sample of new employees to determine that each sampled new hire was subject to background screening procedures.	No exceptions noted.
	The Company has formally documented workforce conduct standards within the Standard of Conduct. Employees are required to acknowledge that they have read and agree to the Standard of Conduct upon hire.	Inspected workforce conduct standards within the Standard of Conduct to determine that they were in place.	No exceptions noted.

CC1.0 Criteria Related to Organization and Management			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
		Inspected acknowledgements for a sample of new hires to determine that employees were required to acknowledge that they had read and agreed to the Standard of Conduct upon hire.	No exceptions noted.

CC2.0 Criteria Related to Communications

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	The Company has prepared a description of the system and its boundaries and provides this description to internal and external authorized users.	Inspected the most recent copy of the Company's system description to determine that the system description was documented and available to authorized internal and external users.	No exceptions noted
	The Company has network and dataflow diagrams that are available to authorized users, upon request.	Inspected network and dataflow diagrams to determine that they were documented and available to authorized users.	No exceptions noted
CC2.2 The entity's commitments relating to the in-scope TSPs are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	The Company has documented the security, availability, and confidentiality requirements and commitments through a suite of comprehensive policies and procedures that are provided to authorized users, including onsite contractors and end-user personnel, via the corporate intranet.	Inspected the Company's policies and procedures to determine that policies were in place and documented the security, availability, and confidentiality requirements and commitments.	No exceptions noted
		Inspected the policies and procedures on the corporate intranet to determine that documented security, availability, and confidentiality policies and procedures were available for employees on the Company's intranet.	No exceptions noted
	The Company's security, confidentiality, and availability commitments are communicated to customers via a standard Master Services Agreement (MSA) and Service Level Agreements (SLAs).	Inspected the standard MSA and SLA templates to determine that security, availability, and confidentiality commitments were communicated to customers.	No exceptions noted.

CC2.0 Criteria Related to Communications

Criteria	Service Organization’s Controls	Service Auditor’s Tests	Results of Tests
CC2.3 The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	As part of the security awareness training program, the Company requires all employees to affirm that they have received and understand the Company's security policies upon hire and annually thereafter.	Inspected security policy acknowledgements for a sample of new hires to determine that employees were required to acknowledge that they had read and agreed to the Company's security policies upon hire.	No exceptions noted.
		Inspected security policy acknowledgements for a sample of employees to determine that employees were required to acknowledge that they had read and agreed to the Company's security policies on an annual basis.	No exceptions noted.
	The Company’s security, confidentiality, and availability commitments are communicated to customers via a standard MSA and SLAs.	Inspected the standard MSA and SLA templates to determine that security, availability, and confidentiality commitments were communicated to customers.	No exceptions noted.
CC2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the in-scope TSPs of the system, is provided to personnel to carry out their responsibilities.	The Company has documented the security, availability, and confidentiality requirements and commitments through a suite of comprehensive policies and procedures that are provided to authorized users, including onsite contractors and end-user personnel, via the corporate intranet.	Inspected the Company's policies and procedures to determine that policies were in place and documented the security, availability, and confidentiality requirements and commitments.	No exceptions noted.
		Inspected the policies and procedures on the corporate intranet to determine that documented security, availability, and confidentiality policies and procedures were available for employees on the Company’s intranet.	No exceptions noted.

CC2.0 Criteria Related to Communications

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
	The Company requires all personnel to undergo security awareness training as part of the on-boarding process and annually thereafter.	Inspected training documentation to determine that security awareness training included development in system security concepts and issues.	No exceptions noted.
		Inspected training completion evidence for a sample of new hires to determine that security awareness training was completed as part of the on-boarding process for each new hire sampled.	No exceptions noted.
		Inspected training completion evidence for a sample of employees to determine that security awareness training was completed for each employee on an annual basis.	No exceptions noted.
CC2.5 Internal and external users have been provided with information on how to report failures, incidents, concerns, and other complaints related to the in-scope TSPs to appropriate personnel.	The Company has developed and distributed security incident response policies and procedures that are communicated to authorized users.	Inspected the security incident response policies and procedures to determine that they were documented and communicated to authorized users.	No exceptions noted
	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of security incident tickets to determine that incidents related to security were logged, tracked, and communicated to affected parties by management until resolved.	No exceptions noted

CC2.0 Criteria Related to Communications

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
	The Company provides an external-facing support system (Datapipe One Portal) allowing users to report system information on failures, incidents, concerns, changes, and other complaints to appropriate personnel.	Observed the customer reporting portal to determine that an external-facing support system was available to users to report system information on failures, incidents, concerns, request changes, and other complaints.	No exceptions noted
CC2.6 System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to the in-scope TSPs are communicated to those users in a timely manner.	System changes are communicated to authorized internal users via a ticketing system.	Inspected tickets for a sample of changes to determine that change information was communicated to authorized internal users in a timely manner via a ticketing system.	No exceptions noted
	The Company notifies user entities of critical changes that may affect their processing.	Inspected evidence for a sample of changes to determine that the Company communicated changes that may affect user's processing.	No exceptions noted

CC3.0 Criteria Related to Risk Management and Design and Implementation of Controls

Criteria	Service Organization’s Controls	Service Auditor’s Tests	Results of Tests
CC3.1 The entity (1) identifies potential threats that could impair system commitments, and system requirements related to the in-scope TSPs (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.	A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted
	A risk assessment is performed on at least an annual basis. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected the most recent risk assessment to determine that threats to security were identified and risks were formally assessed on an annual basis.	No exceptions noted
	The Security team subscribes to industry security bulletins and email alerts and uses them to monitor the impact of emerging technologies on security.	Inspected example security bulletins and email alerts to determine that the Security team subscribed to industry security bulletins and email alerts.	No exceptions noted.

CC3.0 Criteria Related to Risk Management and Design and Implementation of Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
CC3.2 The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.	The Company has documented the security, availability, and confidentiality requirements and commitments through a suite of comprehensive policies and procedures that are provided to authorized users, including onsite contractors and end-user personnel, via the corporate intranet.	Inspected the Company's policies and procedures to determine that policies were in place and documented the security, availability, and confidentiality requirements and commitments.	No exceptions noted.
		Inspected the policies and procedures on the corporate intranet to determine that documented security, availability, and confidentiality policies and procedures were available for employees on the Company's intranet.	No exceptions noted.
	A weekly Change Advisory Board (CAB) team meeting is held in which changes to infrastructure and the associated impact on security are discussed.	Inspected meeting minutes for a sample of weeks during the review period to determine that CAB meetings were conducted around changes to infrastructure and the associated impact on security on a weekly basis.	No exceptions noted.
	Internal network vulnerability scans are performed on a quarterly basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected internal network vulnerability scans for a sample of quarters to determine that internal network vulnerability scans were performed quarterly and remediation plans were developed to address all critical and high vulnerabilities.	No exceptions noted.

CC3.0 Criteria Related to Risk Management and Design and Implementation of Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	Penetration testing is performed on at least an annual basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred on at least an annual basis and a remediation plan was developed to address all critical and high vulnerabilities.	No exceptions noted.

CC4.0 Criteria Related to Monitoring of Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
CC4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to the in-scope TSPs, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
	Internal network vulnerability scans are performed on a quarterly basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected internal network vulnerability scans for a sample of quarters to determine that internal network vulnerability scans were performed quarterly and remediation plans were developed to address all critical and high vulnerabilities.	No exceptions noted.
	Penetration testing is performed on at least an annual basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred on at least an annual basis and a remediation plan was developed to address all critical and high vulnerabilities.	No exceptions noted.
	A log management system is utilized to identify trends that may have a potential impact on the Company's ability to achieve its system security objectives.	Inspected the log management system to determine that logs were analyzed for trends with potential impact on the Company's ability to achieve its system security objectives.	No exceptions noted.

CC4.0 Criteria Related to Monitoring of Controls

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
	On a semi-annual basis, IT security reviews a list of domain administrators with access to deploy software in production and recertifies access. Tickets are created and resolved to remove access for users who have separated or no longer require access.	Inspected the most recent review evidence and change tickets (if applicable) to determine that IT security reviewed a list of domain administrators with access to deploy software in production on a semi-annual basis, recertified access, and created and resolved tickets to remove access where applicable.	No exceptions noted.
	On a semi-annual basis, IT security reviews a list of terminated users to ensure that users do not retain access to critical systems after termination. Tickets are created and resolved to remove access for users who have separated.	Inspected the most recent review evidence and change tickets (if applicable) to determine that IT security reviewed a list of terminated users on a semi-annual basis to ensure that users did not retain access to critical systems after termination and tickets were created and resolved to remove access where applicable.	No exceptions noted.
	On a semi-annual basis, IT security reviews a list of AD Organizational Units (OUs) to verify that role-based access is appropriate based on the user's assigned department responsibilities. Tickets are created and resolved to remove access for users who no longer require access.	Inspected the most recent review evidence and change tickets (if applicable) to determine that IT security reviewed a list of AD OUs on a semi-annual basis to verify that role-based access was appropriate based on the user's assigned department responsibilities and tickets were created and resolved to remove access where applicable.	No exceptions noted.

CC4.0 Criteria Related to Monitoring of Controls

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
	A File Integrity Monitoring (FIM) system is in place, monitors for configuration changes, and alerts administrators when deviations from baseline configurations are detected.	Inspected the tool configurations and example alerts to determine that a FIM system was in place, monitored for configuration changes, and alerted administrators when deviations from baseline configurations were detected.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls

Criteria	Service Organization’s Controls	Service Auditor’s Tests	Results of Tests
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity’s commitments and system requirements as they relate to the in-scope TSPs.	The Company permits remote access to production systems by authorized employees only with two-factor authentication over an encrypted virtual private network (VPN) connection.	Observed a remote login session to determine that two-factor authentication over an encrypted VPN connection was required to remotely access production systems.	No exceptions noted.
	The network, application, servers, and databases require users to authenticate via unique usernames and passwords.	Inspected login attempts to determine that the network, application, servers, and databases required users to authenticate via unique username and password.	No exceptions noted.
	The Company leverages Datapipe Access and Audit Control for the Cloud (DAACC) to federate to client AWS accounts in the Cloud Management System (CMS) without requiring client administrative API keys.	Inspected DAACC diagrams and design documentation and observed the login process from CMS to determine that no client administrative API keys were required for federation.	No exceptions noted.
	Production network passwords are configured to enforce the following parameters: - 8-character minimum - Complexity enabled - 90-day password change	Inspected the production network password configuration to determine that the following parameters were in place: - 8-character minimum - Complexity enabled - 90-day password change	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	In-scope applications require users to authenticate via Single Sign On (SSO). SSO passwords are configured to enforce two-factor authentication.	Inspected the SSO configuration to determine that in-scope applications required users to authenticate via SSO and SSO passwords were configured to enforce two-factor authentication.	No exceptions noted.
	Administrator access to the network, infrastructure components, operating systems, and databases is restricted to authorized personnel.	Inspected system access listings to determine that administrator access to the network, infrastructure components, operating systems, and databases was restricted to authorized personnel.	No exceptions noted.
	Access to remotely administer client production environments is restricted to authorized personnel via a password management application and user activity is logged.	Observed the password management application to determine that access to remotely administer production environments was restricted to authorized personnel and user activity was logged.	No exceptions noted.
	The PCI vStrat platform administrative access is restricted to authorized personnel only.	Inspected Secret Server logical access permissions for the PCI vStrat platform to determine that administrative access was restricted to authorized personnel only.	No exceptions noted.
	Access to customer production environments is restricted to authorized personnel via SANTA.	Inspected a listing of users with access to authenticate to SANTA to determine that access was restricted to authorized personnel with a valid job responsibility.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization’s Controls**	**Service Auditor’s Tests**	**Results of Tests**
		Observed a user login to a customer production environment to determine that access was restricted via SANTA.	No exceptions noted.
CC5.2 New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity’s commitments and system requirements as they relate to the in-scope TSPs. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	A new hire provisioning request is completed by the employee’s manager as part of the on-boarding process and fulfilled by IT administrators. The request documents approval for in-scope systems and applications.	Inspected access requests for a sample of new hires to determine that an access provisioning request was documented, approved by the employee’s manager, and fulfilled by IT administrators for each user sampled as part of the onboarding process.	No exceptions noted.
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected a listing of terminated employees and compared the listing to active user listings to determine that terminated employees did not retain access to the in-scope system and platforms after their separation.	No exceptions noted.
		Inspected termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as part of the termination process.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
CC5.3 Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to the in-scope TSPs.	The network, application, servers, and databases require users to authenticate via unique usernames and passwords.	Inspected login attempts to determine that the network, application, servers, and databases required users to authenticate via unique username and password.	No exceptions noted.
	Production network passwords are configured to enforce the following parameters: - 8-character minimum - Complexity enabled - 90-day password change	Inspected the production network password configuration to determine that the following parameters were in place: - 8-character minimum - Complexity enabled - 90-day password change	No exceptions noted.
	In-scope applications require users to authenticate via SSO. SSO passwords are configured to enforce two-factor authentication.	Inspected the SSO configuration to determine that in-scope applications required users to authenticate via SSO and SSO passwords were configured to enforce two-factor authentication.	No exceptions noted.
CC5.4 Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to the in-scope TSPs.	On a semi-annual basis, IT security reviews a list of domain administrators with access to deploy software in production and recertifies access. Tickets are created and resolved to remove access for users who have separated or no longer require access.	Inspected the most recent review evidence and change tickets (if applicable) to determine that IT security reviewed a list of domain administrators with access to deploy software in production on a semi-annual basis, recertified access, and created and resolved tickets to remove access where applicable.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	On a semi-annual basis, IT security reviews a list of terminated users to ensure that users do not retain access to critical systems after termination. Tickets are created and resolved to remove access for users who have separated.	Inspected the most recent review evidence and change tickets (if applicable) to determine that IT security reviewed a list of terminated users on a semi-annual basis to ensure that users did not retain access to critical systems after termination and tickets were created and resolved to remove access where applicable.	No exceptions noted.
	On a semi-annual basis, IT security reviews a list of AD OUs to verify that role-based access is appropriate based on the user's assigned department responsibilities. Tickets are created and resolved to remove access for users who no longer require access.	Inspected the most recent review evidence and change tickets (if applicable) to determine that IT security reviewed a list of AD OUs on a semi-annual basis to verify that role-based access was appropriate based on the user's assigned department responsibilities and tickets were created and resolved to remove access where applicable.	No exceptions noted.
CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to the in-scope TSPs.	Datapipe Owned Facilities: Access to the data centers are controlled via three-factor authentication, which includes iris scan, PIN entry, and badge swipe, prior to gaining entry.	Observed access for a sample of data centers to determine that three-factor authentication was required to gain entry.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	Datapipe Third-Party Colo Owned Facilities: Access to the Company suites or cages are controlled via multi factor authentication, which includes iris scan and PIN, prior to gaining entry.	Observed access for a sample of data centers to determine that multi-factor authentication was required to gain entry to suites or cages.	No exceptions noted.
	Datapipe Owned Facilities: Predefined physical security zones are utilized to assign role-based access to and throughout the data center.	Inspected the card access zone definition listing to determine that predefined physical security zones were utilized for the assignment of role-based physical access privileges to and throughout the data center.	No exceptions noted.
	The badge access system is configured to create and store an access log for ad hoc review purposes. The access log includes the employee name, date/time, and location.	Inspected badge access system logs for a sample of months during the review period to determine that the access logs were available for ad hoc review purposes and included the employee name, date/time, and location.	No exceptions noted.
	Security personnel revoke the badge access privileges assigned to a terminated employee as a component of the termination process.	Inspected termination tickets for a sample of terminated employees during the review period to determine that badge access was revoked for each employee sampled.	No exceptions noted.
	Security personnel review badge access privileges on a semi-annual basis.	Inspected the badge audit report to determine that badge access to the data center was reviewed within the last six months.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	Surveillance cameras are present at each entrance to the data center and are utilized to record data center activity.	Observed camera locations for a sample of data centers to determine that they were present at each entrance to the data center and utilized to record data center activity.	No exceptions noted.
	Customer/visitor access is scheduled by authorized contacts prior to the granting of access to the data center. Before entering the facility and data center areas, visitors are subject to registration procedures including, but not limited to, the following: - Submitting valid photo identification - Signing a visitor sign-in log - Carrying a visible visitor badge	Observed the visitor access process for a sample of data centers to determine that visitors were authorized prior to entering the facility and required to submit valid photo identification and visitor registration, sign into the visitor sign-in log, and carry a visible visitor badge.	No exceptions noted.
	Visitors are required to be escorted by an authorized employee when accessing the data center.	Observed the visitor access process for a sample of data centers to determine that visitors were required to be escorted by an authorized employee when accessing the data center.	No exceptions noted.
	Datapipe Owned Facilities: The entrance to the data center is equipped with a mantrap that utilizes multiple doors to control user access into the data center.	Observed the data center entrance for a sample of data centers to determine that each data center was equipped with a mantrap that utilized multiple doors to control user access into the data center.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC5.6 Logical access security measures have been implemented to protect against threats related to the in-scope TSPs from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Firewalls are used and configured to prevent unauthorized access. Firewall events are logged and are available for review by the security administrator.	Inspected the firewall configuration to determine that firewalls were in place and configured to prevent unauthorized access and that firewall events were logged and available for review.	No exceptions noted.
	The Company has documented network and system hardening standards.	Inspected network and system hardening standards to determine that they were documented.	No exceptions noted.
	Intrusion detection systems (IDS) are used to provide continuous monitoring of the Company's network and early detection of potential security breaches.	Inspected IDS configurations to determine that continuous monitoring of the Company's network and early detection of potential security breaches were in place.	No exceptions noted.
	Firewall rulesets are reviewed on a semi-annual basis.	Inspected the most recent firewall review to determine that firewall rulesets were reviewed within the past six months.	No exceptions noted.
CC5.7 The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to the in-scope TSPs.	Web communication sessions are encrypted via Transport Layer Security (TLS) to protect communications between the system and users connecting to the system from customer networks.	Inspected TLS settings to determine that transmission of confidential and/or sensitive information between the system and users connecting to the system from customer networks was encrypted via TLS.	No exceptions noted.

CC5.0 Criteria Related to Logical and Physical Access Controls			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	Databases housing sensitive customer data are encrypted at rest.	Inspected database configurations to determine that databases housing sensitive customer data were encrypted at rest.	No exceptions noted.
	The Company permits remote access to production systems by authorized employees only with two-factor authentication over an encrypted VPN connection.	Observed a remote login session to determine that two-factor authentication over an encrypted VPN connection was required to remotely access production systems.	No exceptions noted.
CC5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to the in-scope TSPs.	The Company has deployed anti-malware technology for environments commonly susceptible to malicious attack and has configured it to be updated routinely, logged, and installed on all relevant production servers.	Inspected screenshots of anti-malware software configurations to determine that it was updated routinely, logged, and installed on all relevant production servers.	No exceptions noted.

CC6.0 Criteria Related to System Operations

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC6.1 Vulnerabilities of system components to breaches and incidents related to the in-scope TSPs due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to the in-scope TSPs.	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted
	Internal network vulnerability scans are performed on a quarterly basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected internal network vulnerability scans for a sample of quarters to determine that internal network vulnerability scans were performed quarterly and remediation plans were developed to address all critical and high vulnerabilities.	No exceptions noted.
	Penetration testing is performed on at least an annual basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred on at least an annual basis and a remediation plan was developed to address all critical and high vulnerabilities.	No exceptions noted.
	A FIM system is in place, monitors for configuration changes, and alerts administrators when deviations from baseline configurations are detected.	Inspected the tool configurations and example alerts to determine that a FIM system was in place, monitored for configuration changes, and alerted administrators when deviations from baseline configurations were detected.	No exceptions noted

CC6.0 Criteria Related to System Operations

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC6.2 Incidents related to the in-scope TSPs, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	The Company has developed and distributed security incident response policies and procedures that are communicated to authorized users.	Inspected the security incident response policies and procedures to determine that they were documented and communicated to authorized users.	No exceptions noted
	All incidents related to security are logged, tracked, and communicated to affected parties by management until resolved.	Inspected a sample of security incident tickets to determine that incidents related to security were logged, tracked, and communicated to affected parties by management until resolved.	No exceptions noted

CC7.0 Criteria Related to Change Management

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
CC7.1 The entity's commitments and system requirements, as they relate to the in-scope TSPs, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Formally documented change management procedures are in place to govern the modification and maintenance of production systems and address security, availability, and confidentiality requirements.	Inspected the change management procedures to determine that procedures were in place to govern the modification and maintenance of production systems and addressed security, availability, and confidentiality requirements.	No exceptions noted.
	The Company has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	Inspected the formal SDLC methodology to determine that it governed the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.	No exceptions noted.
	A weekly CAB team meeting is held in which changes to infrastructure and the associated impact on security are discussed.	Inspected meeting minutes for a sample of weeks during the review period to determine that CAB meetings were conducted around changes to infrastructure and the associated impact on security on a weekly basis.	No exceptions noted.
CC7.2 Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to the in-scope TSPs.	The Company has documented the security, availability, and confidentiality requirements and commitments through a suite of comprehensive policies and procedures that are provided to authorized users, including onsite contractors and end-user personnel, via the corporate intranet.	Inspected the Company's policies and procedures to determine that policies were in place and documented the security, availability, and confidentiality requirements and commitments.	No exceptions noted.

CC7.0 Criteria Related to Change Management

Criteria	Service Organization’s Controls	Service Auditor’s Tests	Results of Tests
		Inspected the policies and procedures on the corporate intranet to determine that documented security, availability, and confidentiality policies and procedures were available for employees on the Company’s intranet.	No exceptions noted.
	The Company's policies and procedures are updated on an annual basis to remain consistent with the Company's commitments and system requirements.	Inspected the Company's policies and procedures to determine that they were updated on an annual basis to remain consistent with the Company's commitments and system requirements.	No exceptions noted.
	A risk assessment is performed on at least an annual basis. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected the most recent risk assessment to determine that threats to security were identified and risks were formally assessed on an annual basis.	No exceptions noted.
CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity’s commitments and system requirements as they relate to the in-scope TSPs.	Internal network vulnerability scans are performed on a quarterly basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected internal network vulnerability scans for a sample of quarters to determine that internal network vulnerability scans were performed quarterly and remediation plans were developed to address all critical and high vulnerabilities.	No exceptions noted.

CC7.0 Criteria Related to Change Management

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
	Penetration testing is performed on at least an annual basis. Remediation plans are developed to address all critical and high vulnerabilities.	Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred on at least an annual basis and a remediation plan was developed to address all critical and high vulnerabilities.	No exceptions noted.
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's commitments and system requirements related to the in-scope TSPs.	The Company's advanced change management process requires that infrastructure change requests: - are authorized by management - are formally documented - include documented rollback procedures - are tested - are reviewed and approved by CAB	Inspected change requests for a sample of infrastructure changes that occurred during the review period to determine that infrastructure change requests: - were authorized by management - were formally documented in a change request - Included documented rollback procedures - were tested - were reviewed and approved by CAB	No exceptions noted.
	The Company's application change management process requires that application change requests are: - Formally documented - Tested by QA prior to migration to production - Reviewed and approved by management	Inspected change requests for a sample of application changes that occurred during the review period to determine that application changes were: - Formally documented - Tested by QA prior to migration to production - Reviewed and approved by management	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

A1.0 Additional Criteria for Availability			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
A1.1 Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	An IT infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
	Datapipe Owned Facilities: An environmental monitoring system is in place and configured to monitor and automatically generate an alert to management when predefined environmental thresholds are met.	Inspected environmental monitoring system configurations and an example alert to determine that the system was configured to monitor and automatically generate alerts to management when predefined environmental thresholds were met.	No exceptions noted.
A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Datapipe Owned Facilities: The Company has implemented environmental security measures in the data centers that include smoke detectors, fire suppression systems, water detectors installed within the raised floor areas, uninterruptible power supplies (UPSs), and emergency power supplies.	Observed a sample of data centers to determine that the Company had implemented environmental security measures to include smoke detectors, fire suppression systems, water detectors, UPSs, and emergency power supplies.	No exceptions noted.

A1.0 Additional Criteria for Availability			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
	Datapipe Owned Facilities: Maintenance inspections of fire suppression devices and smoke detectors at Company data centers are performed on an annual basis.	Inspected facility maintenance records of fire suppression devices and smoke detectors at each of the in-scope data centers to determine that inspections were completed on an annual basis.	No exceptions noted.
	Datapipe Owned Facilities: Maintenance inspections of backup generators, HVAC units, and UPS units are performed on a quarterly basis.	Inspected facility maintenance records of backup generators, HVAC units, and UPS units at each of the in-scope data centers to determine that inspections were completed on a quarterly basis.	No exceptions noted.
	An automated backup system is configured to perform daily differential incremental and weekly full backups of client data, unless the frequency is modified by the client.	Inspected the backup configuration to determine that daily differential incremental and weekly full backups were configured for client data by default.	No exceptions noted.
	Disk backups of client data are replicated to an offsite data center on a daily basis.	Inspected database configurations to determine that disk backups of client data were replicated to a secondary offsite data center on a daily basis.	No exceptions noted.
	Backup failures are monitored and email alerts are configured to send to backup administrators. Tickets are created to track and resolve backup issues.	Inspected backup failure alert configurations and example email alerts to determine that alerts were configured to send to backup administrators and tickets were created to track and resolve backup issues.	No exceptions noted.

A1.0 Additional Criteria for Availability			
Criteria	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
A1.3 Recovery Plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	A documented disaster recovery (DR) plan is in place.	Inspected the DR plan to determine that a documented DR plan was in place.	No exceptions noted.
	A DR test is performed at least annually.	Inspected most recent DR test results to determine that a DR test was performed at least annually.	No exceptions noted.
	The Company uses multiple production data centers with significant geographical separation to mitigate the risk of system disruption due to natural disaster or loss of services.	Inspected evidence of redundant data centers to determine that the Company used a multi-location strategy for its production data centers to mitigate the risk of system disruption due to natural disaster or loss of services.	No exceptions noted.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

C1.0 Additional Criteria for Confidentiality

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
C1.1 Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	The Company manages the physical infrastructure and operating system level for customers, but does not perform any changes that would impact customer data/confidential information. Therefore, C1.1 is not applicable.	Not applicable.	Not applicable.
C1.2 Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	Administrator access to the network, infrastructure components, operating systems, and databases is restricted to authorized personnel.	Inspected system access listings to determine that administrator access to the network, infrastructure components, operating systems, and databases was restricted to authorized personnel.	No exceptions noted.
	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access.	Inspected signed confidentiality agreements for a sample of new hires to determine that employees were provided and accepted the agreement as a routine part of their employment.	No exceptions noted.
	The network is segmented to prevent unauthorized access of customer data for managed cloud and PCI vStrat environments.	Inspected the network diagram and network configurations to determine that customer environments and data were segmented for the managed cloud and PCI vStrat environments.	No exceptions noted.

C1.0 Additional Criteria for Confidentiality

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
C1.3 Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access.	Inspected signed confidentiality agreements for a sample of new hires to determine that employees were provided and accepted the agreement as a routine part of their employment.	No exceptions noted.
	Business partners are subject to mutual nondisclosure agreements or other contractual confidentiality provisions.	Inspected nondisclosure agreements for a sample of business partners to determine that business partners signed nondisclosure agreements or other contractual confidentiality provisions.	No exceptions noted.
	Web communication sessions are encrypted via TLS to protect communications between the system and users connecting to the system from customer networks.	Inspected TLS settings to determine that transmission of confidential and/or sensitive information between the system and users connecting to the system from customer networks was encrypted via TLS.	No exceptions noted.
	The Company permits remote access to production systems by authorized employees only with two-factor authentication over an encrypted VPN connection.	Observed a remote login session to determine that two-factor authentication over an encrypted VPN connection was required to remotely access production systems.	No exceptions noted.
	Databases housing sensitive customer data are encrypted at rest.	Inspected database configurations to determine that databases housing sensitive customer data were encrypted at rest.	No exceptions noted.

C1.0 Additional Criteria for Confidentiality

Criteria	Service Organization’s Controls	Service Auditor’s Tests	Results of Tests
C1.4 The entity obtains confidentiality commitments that are consistent with the entity’s confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	Business partners are subject to mutual nondisclosure agreements or other contractual confidentiality provisions.	Inspected nondisclosure agreements for a sample of business partners to determine that business partners signed nondisclosure agreements or other contractual confidentiality provisions.	No exceptions noted.
C1.5 Compliance with the entity’s confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	The Company obtains representations and assurances about the controls that are followed by third-party data centers and obtains a report on the effectiveness of such controls from the data centers’ independent auditor.	Inspected evidence of attestation report review for the third-party data centers to determine that the data center attestation reports were reviewed.	No exceptions noted.
	Vendor risk assessments are conducted during the vendor on-boarding process to evaluate compliance with confidentiality commitments and requirements of vendors and other third parties whose products and services comprise part of the Company system.	Inspected evidence that vendor risk assessments were conducted during the vendor on-boarding process to determine that they evaluated compliance with confidentiality commitments and requirements of vendors and other third parties whose products and services comprise part of the Company system.	No exceptions noted.

C1.0 Additional Criteria for Confidentiality

Criteria	Service Organization's Controls	Service Auditor's Tests	Results of Tests
C1.6 Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	Changes to confidentiality provisions in third-party service provider contracts are renegotiated with the service provider by the legal department. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. There were no changes to confidentiality provisions in third-party service provider contracts during the period.	Inquired of management to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. There were no changes to confidentiality provisions in third-party service provider contracts during the period.
C1.7 The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	Data is retained in accordance with customer and legal requirements.	Inspected the retention policy and data records to determine that data was retained in accordance with customer and legal requirements.	No exceptions noted.
	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of the Company's and customers' data.	Inspected data retention and disposal procedures to determine that they were in place.	No exceptions noted.
C1.8 The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of the Company's and customers' data.	Inspected data retention and disposal procedures to determine that they were in place.	No exceptions noted.

C1.0 Additional Criteria for Confidentiality

Criteria	Service Organization’s Controls	Service Auditor’s Tests	Results of Tests
	Electronic media containing confidential information is purged or destroyed in accordance with best practices and certificates of destruction are issued for each device destroyed.	Inspected certificates of destruction for a sample of media destroyed during the review period to determine that the Company tracked and properly disposed of sensitive media.	No exceptions noted.
	Customer data containing confidential information is purged or removed from the environment, in accordance with best practices, when customers leave the service.	Inspected tickets for data removal for a sample of customers who left the service during the review period to determine that customer data containing confidential information was purged or removed from the environment when customers left the service.	No exceptions noted.