REPORT ON DATAPIPE, INC.'S DESCRIPTION OF ITS DATA CENTER HOSTING SERVICES AND ASPECTS OF GLOBAL SWITCH'S DATA CENTER HOSTING SERVICES AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

April 1, 2017 to March 31, 2018

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Datapipe, Inc. ("Datapipe")

SCOPE

We have examined Datapipe and Global Switch's description of their Data Center Hosting Services entitled "Description of Datapipe's Data Center Hosting Services and Aspects of Global Switch's Data Center Hosting Services for the Period April 1, 2017 to March 31, 2018" (description), and the suitability of the design and operating effectiveness of Datapipe's and Global Switch's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in Datapipe's assertion and Global Switch's assertion (assertions). Global Switch is a subservice organization that provides colocation services to Datapipe. Datapipe's description includes a description of Global Switch's Data Center Hosting Services used by Datapipe, including controls relevant to the control objectives stated in the description. The controls and control objectives included in the description are those that management of Datapipe and Global Switch believe are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Data Center Hosting Services that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Datapipe's and Global Switch's controls are suitably designed and operating effectively, along with related controls at the service organization and the subservice 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.

SERVICE ORGANIZATION'S RESPONSIBILITIES

In Section 2 of this report, Datapipe and Global Switch have provided their assertions about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Datapipe and Global Switch are responsible for preparing the description and their assertions, including the completeness, accuracy, and method of presentation of the description and assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertions, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

SERVICE AUDITOR'S RESPONSIBILITIES

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements (ISAE) 3402, "*Assurance Reports on Controls at a Service Organization*," issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertions, the description is fairly presented and the controls were suitably designed and

operating effectively to achieve the related control objectives stated in the description throughout the period 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 –

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

SERVICE AUDITOR'S INDEPENDENCE AND QUALITY CONTROL

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

INHERENT LIMITATIONS

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

DESCRIPTION OF TESTS OF CONTROLS

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 of this report.

OPINION

In our opinion, in all material respects, based on the criteria described in Datapipe's and Global Switch's assertions -

a. the description fairly presents Datapipe's Data Center Hosting Services and Global Switch's Data Center Hosting Services used by Datapipe that were designed and implemented throughout the period April 1, 2017 to March 31, 2018.

b. the controls of Datapipe and Global Switch related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2017 to March 31, 2018, and user entities applied the complementary controls assumed in the design of Datapipe's and Global Switch's controls throughout the period April 1, 2017 to March 31, 2018.

c. the controls of Datapipe and Global Switch operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2017 to March 31, 2018 if complementary user entity controls assumed in the design of Datapipe's and Global Switch's controls operated effectively throughout the period April 1, 2017 to March 31, 2018.

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 Data Center Hosting Services during some or all of the period April 1, 2017 to March 31, 2018, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Coalfire Controls LLC

May 25, 2018
Louisville, Colorado

SECTION 2

MANAGEMENT'S ASSERTIONS

Assertion of the Management of Datapipe, Inc.

We have prepared the description of Datapipe, Inc.'s Data Center Hosting Services System and aspects of Global Switch's Data Center Hosting Services for the period April 1, 2017 to March 31, 2018 (description) for user entities of the system during some or all of the period April 1, 2017 to March 31, 2018, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves when assessing the risks of material misstatements of user entities' financial statements.

Datapipe, Inc. uses Global Switch, a subservice organization, to provide data center hosting services. Datapipe, Inc.'s description includes a description of Global Switch's Data Center Hosting Services used by Datapipe, Inc., including controls relevant to the control objectives stated in the description. Global Switch's assertion is presented in Section 2.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Datapipe, Inc.'s and Global Switch'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 Data Center Hosting Services made available to user entities of the system during some or all of the period April 1, 2017 to March 31, 2018 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making our assertion were that the description:

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

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

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

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

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

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

        vi) The services performed by Global Switch, including how the inclusive method has been used in relation to them.

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

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

    b) Includes relevant details of changes to the Data Center Hosting Services during the period covered by the description.

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

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period April 1, 2017 through March 31, 2018 to achieve those control objectives if user entities applied the complementary user entity controls assumed in the design of Datapipe, Inc.'s and Global Switch's controls throughout the period April 1, 2017 to March 31, 2018. The criteria we used in making this assertion were that:

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

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

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

Datapipe, Inc. Authorized Representative

Michael Bross, General Counsel
Title

Global Switch House
3 Nutmeg Lane
London E14 2AX
United Kingdom

T +44 (0)20 7473 9000
globalswitch.com

Assertion of the Management of Global Switch Estates 2 Limited

We are responsible for the portion of the description of Datapipe's and Global Switch Estates 2 Limited's ("Global Switch") Data Center Hosting and Managed Services system entitled "Datapipe's Description of the Data Center Hosting and Managed Services System," for Data Center Hosting services throughout the period April 1, 2017 to March 31, 2018 (description) for the period April 1, 2017 to March 31, 2018, that describes the Data Center Hosting services we provided to Datapipe throughout that period. The description is intended for user entities of the system during some or all of the period April 1, 2017 to March 31, 2018, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Datapipe's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

1) Our portion of the description fairly presents the Data Center Hosting services that Global Switch made available to Datapipe and user entities of the system during the period April 1, 2017 to March 31, 2018 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making our assertion were that the description:

   a) Presents how the Data Center Hosting services' portion of the system made available to Datapipe and user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

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

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

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

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

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

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

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

b) Includes relevant details of changes to the Data Center Hosting and Managed Services system during the period covered by the description.

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

2) The controls related to the control objectives stated in our portion of the description were suitably designed and operating effectively throughout the period April 1, 2017 to March 31, 2018 to achieve those control objectives if user entities applied the complementary controls assumed in the design of Global Switch's controls throughout the period April 1, 2017 to March 31, 2018. The criteria we used in making this assertion were that:

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

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

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

Authorized Representative

GROUP DIRECTOR UK

Title

SECTION 3

DESCRIPTION OF DATAPIPE'S DATA CENTER HOSTING SERVICES AND ASPECTS OF GLOBAL SWITCH'S DATA CENTER HOSTING SERVICES FOR THE PERIOD APRIL 1, 2017 TO MARCH 31, 2018

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 thirteen data centers operating worldwide in the following locations: Somerset, New Jersey, San Jose, California, Ashburn, Virginia, Keflavik, Iceland, London, United Kingdom, Hong Kong, China, and Singapore.

DESCRIPTION OF SERVICES PROVIDED

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 (POU) 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, and security panels.

- Cabinets: a closed structure that houses servers typically made of metal with rails, grounding studs, and interior shelving.

Network Availability

Datapipe provides colocation customers with direct connectivity to the Datapipe network, backed by service level agreements (SLA) that guarantees 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

The London One facility provides the following networking capabilities:

- Connections to geographically available Tier 1 providers
- Peering connections with over 200+ peers at major peering exchange
- Dedicated 1 OGB ring between United Kingdom sites with diverse paths and full redundancy
- Additional bandwidth wave from Slough, United Kingdom
- Encrypted MPLS connectivity to other Datapipe data centers
- Full support for fiber channel and Ethernet hand-offs

User entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize,

record, process, and report transactions processed within the data center services system; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

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.

Boundaries of the System

The scope of this report includes Datapipe's data center services located at the Somerset, New Jersey, San Jose, California, and Global Switch Holdings Limited's (Global Switch) data center hosting services located in London, United Kingdom. Specifics for the data center facilities included within the scope of this report 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 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 18 inch 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 power distribution units (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) I 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, UPS maintenance bypass breakers, are monitored by the BMS, and their status is shown on the active one-line diagram as to its operational status. Load data shall be shown on the active one-line diagram from data captured at the various components of the power system that has 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 inch 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 1 MW 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.

London One (London, United Kingdom)

HVAC

Server rooms are maintained at a controlled temperature of 22 degrees Celsius, plus or minus 2 degrees, and relative humidity is maintained at 50%, plus or minus 10%, as measured by the average of all the environmental sensors throughout the space. The environment is maintained by utilizing the following:

- Chilled water cooling system
- Minimum N+2 resilience on all systems, except CRAC units as noted below
- 35.2MW of total cooling provision
- Diverse distribution pipework throughout the data center facility
- CRAC units within customer areas provided at minimum N+1
- Hot/cold aisles with hot aisle containment

London One is configured with a total of twenty-eight air cooled packaged water chillers, with sixteen rated at 1,500kW and twelve rated at 1,250kW. The resilience is based upon N+4 and they are configured into four zones (North East, South East, South West, and North West) of seven chillers to provide N+1 resilience per zone. Total cooling capacity is twelve at 1,250kW plus twelve at 1,500kW, which equates to 33MW total capacity. The chilled water zones are linked by a common ring at roof level and primary pumps are based upon the four zones having a resilience of N+2 per zone, which equates to twelve pumps in total. Two diversified chilled water circuits drop either side of the building to serve every floor.

At each floor, a pair of connections, north and south, connect to a secondary ring on each floor. Each side of the building has two pumps based upon a resilience of N+N. In normal operation mode, one pump from either side operates under a worst-case scenario to provide 50% of the floor cooling capacity. In a worst-case scenario, should both pumps fail on the north or south system, both pumps on the remaining side of the system are configured to run. The pipework on every floor has been sized for this eventuality and can support 100% flow with a maximum capacity of approximately 3.1 MW. CRAC units for tenants' areas are connected to the on-floor pipework loop and are capable of being served by either riser, thereby offering maximum resilience to each floor.

Fire and Water Damage Detection and Mitigation

London One utilizes dual inter-locking pre-action systems, requiring two smoke heads to be triggered before the gas discharge is initiated. Wet suppression is deployed in common areas only. 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.

Leak detection tape loops are deployed in all areas, above and below floor level. An Automatic Building Management System (ABMS) 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 700-millimeter (mm) minimum raised flooring to keep the customer equipment above the sub floor, and away from any potential liquids. 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 London One facility has been designed to provide redundant reliable power utilizing the following:

- 132kV utility supply with N+1 redundancy
- Utility power supply capacity of 43 mega volt-ampere (MVA)
- Additional utility power supply capacity of 40MVA available
- Technical and mechanical power supplied by onsite DRUPS systems
- 28.3MW technical power

The London One facility is fed from two 132kV incoming supplies from two diverse and separate network power stations. Building load is supported by a total of thirty-seven DRUPS systems in a minimum of N+1 configuration. Power is distributed throughout the building via four power stations supporting 11 kV rings to each floor. The cooling infrastructure is supported by its own standalone power station, allowing maintenance to be performed without interruption to the IT load. Power is supplied to customer IT areas by locally sited PDUs offering A+B outlets to each customer rack.

The DRUPS systems are fueled from at least four 120,000-liter diesel tanks located on site. The DRUPS systems are tested weekly. In the event of a loss of incoming power from the national, the DRUPS systems are capable of supporting building load for approximately 48 hours before requiring refueling. Three separate fuel contracts are in place with a guaranteed response time of eight hours at a maximum. The DRUPS systems will automatically support full building load should there be a loss of incoming supply and the DRUPS engines will take the load within 15 seconds.

All elements of the electrical infrastructure are monitored locally through the site Schneider power monitoring system (PMS). Site staff reacts to any alarms raised as appropriate with the original equipment manufacturers' (OEM) available on call as required.

Security

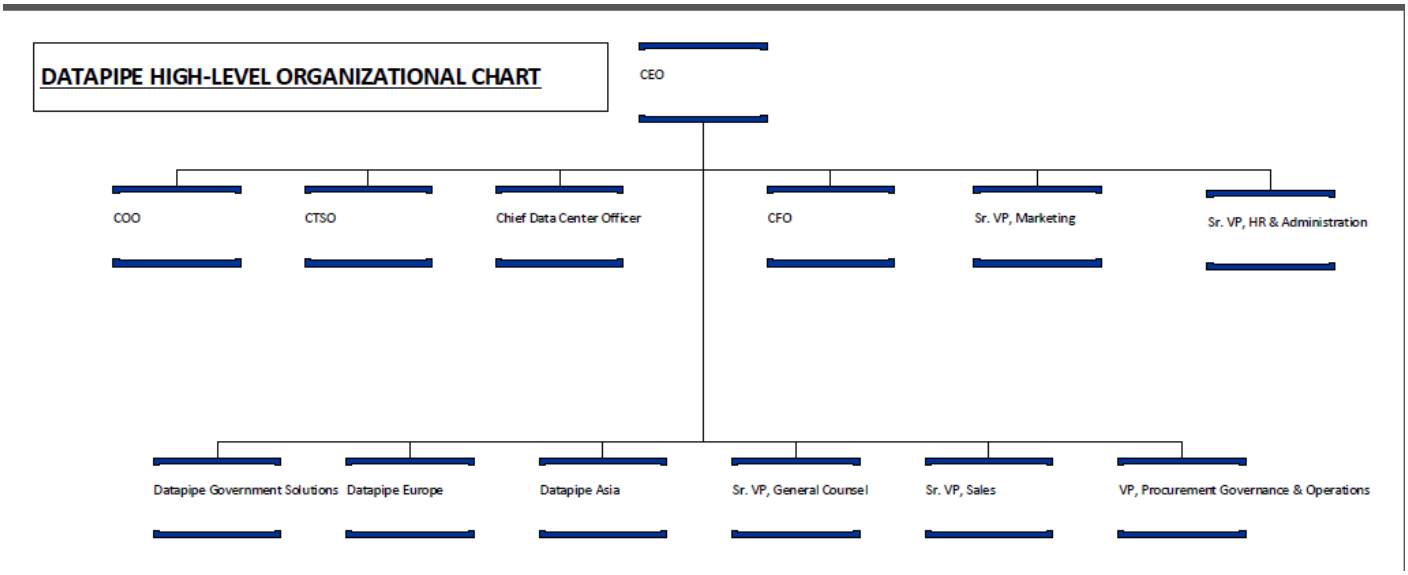
Facility security is maintained by utilizing smartcard readers, mantraps at main entrances to the facility, two-factor authentication to enter Datapipe's private suites, 24 hour per day facility monitoring, and 24 hour per day security staff. The facility is also under 24 hour per day internal and external video surveillance and video is retained for a minimum of 90 days for the Datapipe suites; 30 days for all other monitored areas. Visitors are escorted by authorized personnel at all times.

User entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within the data center services; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Customers are responsible for submitting incidents or requests via e-mail or through the ticketing system. Customer requests are addressed by data center management and are managed according to established SLA.

FUNCTIONAL AREAS OF OPERATIONS

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



- 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

SYSTEM TRANSACTIONS AND REPORTING

User entities are responsible for the procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within the Datapipe Data Centers; this includes the correction of incorrect information and how information is transferred to reports and other information prepared for those user entities.

SUBSERVICE ORGANIZATIONS

Global Switch manages and operates aspects of the data center services to the two Datapipe colocation suites in the London One facility. These services include the physical safeguarding of IT Infrastructure to help ensure that unauthorized access to the IT infrastructure does not occur. Additionally, Global Switch is responsible for providing environmental safeguards (e.g. power supply, temperature control, fire suppression, etc.) against certain environmental threats.

CAPTURING SIGNIFICANT EVENTS AND CONDITIONS

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
- CTSO

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

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.

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 the integrity and ethical values of personnel, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by 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 Datapipe's 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 practices. 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 are described below.

- 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.

Executive Management Oversight

Datapipe's control consciousness is influenced by their executive management. Attributes include executive management' 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. Executive management is in place to oversee management activities and to monitor management's compliance with the entity's objectives.

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.

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 are described below.

- 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.

Accountability

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.

Datapipe's Human Resources (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 are described below.

- 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.

Risk Identification

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 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

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

Risk Analysis

The risk assessment 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.

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.

Integration with Control Objectives

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.

MONITORING

Monitoring Activities

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.

New Jersey One and New Jersey Two

Datapipe monitors the Security Systems 24 hour per day using multiple processes. ABMS 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 Somerset facility emergency action manuals.

Ongoing Monitoring

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 Somerset 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.

Silicon Valley One

Datapipe monitors the Security Systems 24 hours 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 to the San Jose facility emergency action manual.

Ongoing Monitoring

Servers are monitored by Datapipe's custom built observer application. Alerts are escalated in accordance with the customer's SEAP, which is tailored to each customer's solution. Responses are also dictated by the San Jose facility emergency action manual 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.

London One

A Trend 365 BMS is utilized to monitor all environmental controls within the building including temperature and relative humidity in customer IT areas. CRAC units are connected to the BMS and can be locally controlled in the event of local alarms being produced. The 24 hour per day onsite facilities team reacts to any alarms raised and provides local attendance as required. The facilities team is comprised of locally based electrical and mechanical engineers. OEMs are available on call as required. Each shift is led by member of the Global Switch facilities team. All mechanical and electrical equipment is subject to a planned preventive maintenance (PPM) schedule with regular maintenance performed in line with manufacturer's recommendations.

Ongoing Monitoring

Servers are monitored by Datapipe's custom built observer application. Alerts are escalated in accordance with the customer's SEAP, which is tailored to each customer's solution. Responses are also dictated by Global Switch escalation processes and the customer's EAP. These responses are tracked via separate ticketing systems, with unlimited historical tracking.

Policies and procedures exist to support the facility's physical security. This includes procedures for enrollment and review. All individuals entering the facility must be authorized to do so, and they are issued temporary badges.

Separate Evaluations

Datapipe undergoes an ISO 27001 certification assessment annually by a third-party auditor.

Monitoring of Subservice Organizations

Datapipe relies on Global Switch's ISO 27001 annual assessment and certification for comfort over third party control processes.

Reporting Deficiencies

New Jersey One and New Jersey Two

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 Somerset post orders. Additionally, officers shall escalate to the following individuals:

- Security site supervisor
- Data center operations manager
- CTSO

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 Somerset 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

Silicon Valley One

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 Somerset post orders. Additionally, officers shall escalate to the following individuals:

- Security site supervisor
- Data center operations manager
- Chief security officer

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 San Jose facility emergency action manual provides 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

London One

Physical Breach

Should there be a serious incident involving a physical breach of security, officers are instructed to contact the site security manager, who will follow the appropriate recorded protocol for the nature of the

incident. The operations manager is advised of any security breach and escalates to the site managing director (MD), if required for further action.

Should a physical breach directly or indirectly cross impact Datapipe's suites, the director of operations will be notified by Global Switch. In turn, this individual will escalate to the CTSO, CDCO, COO, 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, the Global Switch facilities team will provide the relevant response to the nature of the incident. Where appropriate, customers are advised of the actions taken and any remedial activities that may be required. Local escalation is performed to the facility manager in the first instance, followed by the operations manager and the site MD if appropriate. Global Switch maintains incident management and escalation procedures.

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

Additionally, Global Switch provides Datapipe with a monthly report detailing the environmental conditions maintained throughout the relevant period, recorded against the SLA between Datapipe and Global Switch. The report also contains details of the PPM schedule for Datapipe's leased space.

INFORMATION AND COMMUNICATION

Relevant Information

New Jersey One and New Jersey Two

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

Silicon Valley One

The infrastructure is comprised of multiple bandwidth providers with 1 GB and 20 GB connections to the network. Datapipe runs 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 HSRP for redundant uplinks to two different switches, BGP full routing tables with proper customer provided advertisement, and 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

London One

The infrastructure is comprised of multiple bandwidth providers with 1 GB and 10 GB connections to the network. Datapipe runs 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 HSRP for

redundant uplinks to two different switches, BGP full routing tables with proper customer provided advertisement, and 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
- Trend 365 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

Management is involved with day-to-day operations and provides personnel with an understanding of their individual roles and responsibilities and the relation of individual functions to the overall support of services. Datapipe's management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

Datapipe's organizational structure helps facilitate communication flow by grouping service offerings. Each individual group has a preferred method of communication (e.g., including sales portals, bulletins, etc.). Company-wide communications are facilitated using e-mails, the intranet, and portals. The structure facilitates the flow of information upstream, downstream, and across all business activities.

CONTROL OBJECTIVES AND RELATED CONTROLS

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, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of Datapipe evaluate the relationships between business processes and the use of technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Datapipe personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that

are components of those processes. After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed, and improved when necessary.

Datapipe's control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

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

CONTROL OBJECTIVE 1: PHYSICAL SECURITY

Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

New Jersey One and New Jersey Two

The entranceways to the data center facilities in Somerset, New Jersey, are protected with a smartcard reader which requires an individual to scan their badge at the outermost door. Once inside the vestibule, there are waiting rooms where a third-party security officer sits behind a bullet resistant glass area where they monitor personnel going into and out of the facility. Allied Barton Security Services is contracted to manage and monitor physical access to the data center facilities. Security personnel are staffed 24 hours per day to monitor physical security controls to the data centers. To gain entry through the main data center portals, enrolled individuals require three-factor authentication. Employees, permanent contractors, and enrolled customers are issued printed photo smartcards. These smartcards are color-coded so as to be able to easily identify facility visitors, customers, staff, and contractors. When entering the facility, a pop-up of the enrolled individual's picture appears on the security officer's computer screen for a visual confirmation.

Visitors and temporary contractors must first use the phone outside the facilities to signal the officer to allow them entry into the waiting area. They must then surrender government issued picture identification or vendor identification in specific cases to the officer and sign in via the appropriate log before the officer issues them a temporary smartcard. The smartcard can then be swiped to allow escorted entry into the mantraps in accordance with the procedures below.

For the New Jersey One data center, an enrolled individual must enter their six-digit personal identification number (PIN) to activate the iris scanner and confirm their identity. A successful iris verification will enable the smartcard reader. All individuals, including enrollees and visitors, must individually swipe their smartcard before entering the single man security portal. The timed anti-passback security feature is enabled on this reader, preventing one individual from swiping their badge multiple times in attempt to allow multiple individuals to enter. A green light on the portal will illuminate to indicate the individual is authorized and may enter. Sensors in the floor of the portal will detect if there are more than one person present, or if an individual has entered the portal without a valid smartcard swipe. If an unauthorized entry is detected, the outer door will remain open and will not allow the unauthorized individual to proceed. Once the outer door is closed, the inner portal door will automatically open assuring that both doors are never opened at the same time.

For the New Jersey Two data center, an enrolled individual must enter their six-digit PIN to activate the iris scanner and confirm their identity. Successful iris verification will enable the smartcard reader. All

individuals, including enrollees and visitors, must then swipe their smartcard for authorization to signal the security portal to rotate in order to permit entry. The timed anti-passback security feature is enabled on this reader, preventing one individual from swiping their badge multiple times in attempt to allow multiple individuals to enter. Weight sensors inside of the portal detect entering and exiting individuals. If an unauthorized entry is detected, such as an individual attempting to gain entry without a valid card swipe while the portal is rotating to allow someone to exit, an audible alarm will sound and the security portal will reverse its rotation forcing the unauthorized individual to exit the portal.

A similar process of PIN and iris scan authentication in a mantrap configuration is repeated for entry into the internal managed services server rooms; however, independent doors allowing multiple people to enter simultaneously are employed. Due to this configuration, there is a secondary smartcard reader inside of the mantrap, which will only be activated after the first door has closed. All smartcard swipes are logged and reviewed by data center personnel on an ad hoc basis. Physical access smartcards have an expiration date set in the software to expire six months from issuance. At that point, a review process is conducted to help ensure that individual's role and additional access is still appropriate. Role-based access is reviewed semi-annually by department managers and/or executives. Datapipe personnel access to the colocation areas is restricted to authorized personnel. Upon receipt of an access revocation request ticket from executive management, human resources, the facility manager or the customer, smartcards are immediately deactivated by the security department by setting the expiration date to the termination date. Administrative access to the card access and biometric access systems are restricted to authorized personnel.

Internal door physical keys are maintained and managed by data center management and security officers. Security personnel require an authorized key request form before issuing permanent and temporary keys. The security office has a restricted box that contains emergency keys, which is monitored and logged.

Data center security personnel require an authorized ticket be submitted prior to granting tour members, temporary contractors, or visitors' access to the data center, indicating the date and time of their visit. Permanent contractors are enrolled into the access control system and issued a smartcard. Permanent contractors must be approved via ticket by authorized Datapipe personnel.

Video cameras are placed in external areas and all built-out areas inside the facilities. Video monitoring is done at the officer's stations, and the surveillance system provides full coverage of all colocation server rooms and throughout the data centers. Video recordings are archived for at least 90 days and reviewed on an ad hoc basis.

Silicon Valley One

The entranceway to the data center facility in San Jose, California, requires an individual to scan their badge at the outermost door. Once inside the vestibule, individuals are required to authenticate via a three-factor authentication system. An enrolled individual must enter their six-digit PIN to activate the iris scanner and confirm their identity. A successful iris verification will enable the smartcard reader. After authentication, the mantrap opens and only allows one person to enter the data center facility at a time. A third-party security officer sits behind a bullet resistant glass area where they monitor personnel going into and out of the facility. AlliedBarton Security Services is contracted to manage and monitor physical access to the data center. Security personnel are staffed 24 hours per day to monitor physical security controls to the data center. For visitors to gain entry to the facility, the security personnel obtain a government issued ID from the individual and keep it until the person leaves the facility. Employees, permanent contractors, and enrolled customers are issued printed photo smartcards. These smart cards

are color-coded so as to be able to easily identify facility visitors, customers, staff and contractors. When entering the facility, a pop-up of the enrolled individual's picture appears on the security officer's computer screen for a visual confirmation.

After entering the main facility door, individuals are then required to authenticate again at the main data center door. Behind this door are all employee areas (offices, facilities workshop, break room, etc.). To gain access, an enrolled individual must authenticate via the iris scanner and scan their badge at the smartcard reader. Beyond the main data center door, access to the standard colocation suites is accomplished by scanning your smartcard. To access the managed services suites, personnel must authenticate using the iris scanner and the smartcard reader. Mantrap systems are in place as well. These mantraps allow multiple people to enter simultaneously; due to this configuration, there is a secondary smartcard reader inside of the mantrap, which will only be activated after the first door has closed. All smartcard swipes are logged and reviewed by data center personnel on an ad hoc basis. Physical access smartcards have an expiration date set in the software to expire six months from issuance. At that point, a review process is conducted to help ensure that individual's role and additional access is still appropriate. Role-based access is reviewed semi-annually by department managers and/or executives for appropriateness.

Datapipe personnel access to the colocation areas is restricted to authorized personnel. Upon receipt of an access revocation request ticket from executive management, human resources, the facility manager or the customer, smartcards are immediately deactivated by the security department by setting the expiration date to the termination date. Administrative access to the card access and biometric access systems are restricted to authorized personnel.

Internal door physical keys are maintained and managed by data center management and security officers. Security personnel require an authorized key request form before issuing permanent and temporary Mul-T-Lock keys. The security office has a restricted box that contains emergency keys, which is monitored and logged. Additionally, customer cage keys are maintained and managed by the data center operations supervisor. Once a key request form is properly documented and approved by security personnel, customers are issued unique locks and keys for their individual cages.

Data center security personnel require an authorized ticket be submitted prior to granting tour members, temporary contractors, or visitors' access to the data center, indicating the date and time of their visit. Permanent contractors are enrolled into the access control system and issued a smartcard. Permanent contractors must be approved via ticket by authorized Datapipe personnel.

Video cameras are placed in external areas and all built-out areas inside the facility. Video monitoring is done at the officer's station, and the surveillance system provides full coverage of all colocation server rooms and throughout the entire data center. Video recordings are archived for at least 90 days and reviewed on an ad hoc basis.

London One

The entrance to the Global Switch Data center in London, UK is protected with a smartcard reader. At the entrance to the data center, there is a waiting room with a Global Switch security officer behind bullet resistant glass. Global Switch is contracted to manage and monitor physical access to the data center. Security personnel are staffed 24 hours per day to monitor physical security controls to the data center.

Any individual that has been enrolled in the Global Switch system and issued a badge must swipe their badge to enter either one of the two side-by-side mantraps / portals to enter the data center waiting room / lobby area. Sensors in the floor of the portal will detect if there is more than one person present, or if an individual has entered the portal without a valid smartcard swipe. If an unauthorized entry is detected, the outer door will remain open and will not allow the unauthorized individual to proceed. Once the outer door is closed, the inner portal door will automatically open assuring that both doors are never opened at the same time. Card swipes are utilized to exit the facility as well.

Visitors must use the portal with the intercom to contact the security office and obtain entry. Security staff members will review one of two lists for the visitor's name: the 24 hour per day access list for all Datapipe employees and/or the visitor access list for colocation customers and infrequent or one-time visitors. Both groups require an escort at all times. All un-enrolled individuals must sign the visitor log book and are then given a temporary badge once their photo identification has been inspected by the security staff member. Badge access is required to gain access to the elevator and each of the floors, and provides individuals with access to the shared corridors, based on the role based badge access levels. Datapipe has implemented its own access control system to protect its suites, which are completely independent from Global Switch's other suites. Global Switch does not have access to the Datapipe suites and must be escorted at all times by authorized Datapipe personnel if they are required to enter the Datapipe suites. The access control system for the Datapipe suites utilizes two-factor authentication in the form of a PIN and iris scanner. An authorized individual must enter their six-digit PIN (minimum) to activate the iris scanner and confirm their identity. Successful iris verification and adequate authorization within the access control system will allow access to the Datapipe suites. All access attempts are logged and reviewed on an ad hoc basis by data center personnel in the Datapipe San Jose, California facility.

Data center security personnel require an authorized ticket be submitted prior to granting tour members, temporary contractors, or visitors' access to the data center, indicating the date and time of their visit. Permanent contractors are enrolled into the access control system and issued a smartcard. Permanent contractors must be approved via ticket by authorized Datapipe personnel.

Global Switch places video cameras in internal and external common areas. These cameras are monitored 24 hours per day in the Global Switch security control room, and the video recording is archived for 30 days for ad hoc review purposes by security personnel. For the Datapipe suites, video cameras are placed in suite entrances / exits and various built-out aisles inside the suites. Video monitoring is done at an officer's station in the Datapipe Somerset, New Jersey facility. Video recording is archived for at least 90 days and reviewed on ad hoc basis.

Physical access smartcards have an expiration date set in the software to expire six months from issuance. At that point, a review process is conducted to help ensure that individual's role and additional access is still appropriate. Role-based access is reviewed semi-annually by department managers and/or executives. Datapipe personnel access to the colocation areas is restricted to authorized personnel. Upon receipt of an access revocation request ticket, smartcards are immediately deactivated by the security department by setting the expiration date to the termination date. Administrative access to the card access and biometric access systems are restricted to authorized personnel.

CONTROL OBJECTIVE 2: ENVIRONMENTAL SECURITY

Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

New Jersey One and New Jersey Two

Documented policies and procedures are in place to guide employees in the maintaining and monitoring of the environmental equipment supporting the data centers. The data centers are designed with redundancy for key systems, including Internet data connections, core routers, access and distribution switches, CRAC units, UPS, POU, and generators.

All backup power systems are capable of maintaining continuous system services to the data centers for at least 72 hours without additional fuel. Two independent diesel contractors help ensure delivery before supplies are exhausted.

Processes and systems are implemented to prevent, detect, and mitigate fire damage. The data centers are equipped with multi-zoned fire suppression systems, aspirating smoke detectors, heat detectors, fire alarms, fire extinguishers and single interlocking dry-pipe pre-activation sprinkler systems. Fire drills are completed at least annually to help ensure fire alarms are operating as intended. In regards to leak prevention, 18 inch raised flooring and leak detection systems are utilized in the data server rooms.

Environmental systems are inspected and preventive maintenance is performed at regular intervals. The CRAC units and generators are inspected on a quarterly basis, while the fire suppression / detection systems, PDUs, UPS systems, and leak detection systems are inspected on a semi-annual or annual basis. Environmental controls are monitored by the data center engineering team 24 hours per day using the BMS. The BMS is configured to send e-mail alert notifications to IT personnel in the event of a device failure and when predefined thresholds are exceeded for certain environmental factors. System events are documented, recorded, and escalated as required. If the problem cannot be immediately resolved by the data center engineering team, it is then escalated to the data center operations manager for further investigation. The data center engineering department has documented escalation procedures for each data center.

Additionally, security personnel conduct facility rounds, which include checking environmental control panels and documenting, recording, and escalating system events as required. An incident tracking system is in place to document, record, and escalate environmental system events to help ensure issues are resolved and resolution steps are documented.

Silicon Valley One

Documented policies and procedures are in place to guide employees in the maintaining and monitoring of the environmental equipment supporting the data center. The data center is designed with redundancy for key systems, including Internet data connections, core routers, access and distribution switches, CRAC units, UPS / DRUPS systems, and PDUs.

Backup power systems are capable of maintaining continuous system services to the entire data center for at least 48 hours without additional fuel. Two independent diesel contractors help ensure delivery before supplies are exhausted. Processes and systems are implemented to prevent, detect, and mitigate fire damage. The data center is equipped with multi-zoned fire suppression systems, aspirating smoke detectors, heat detectors, fire alarms, fire extinguishers and single interlocking dry-pipe pre-activation sprinkler systems. Fire drills are completed at least annually to help ensure fire alarms are operating as

intended. In regards to leak prevention, 18 inch raised flooring and leak detection systems are utilized in the data server rooms.

Environmental systems are inspected and preventive maintenance is performed at regular intervals. The CRAC units and DRUPS systems are inspected on a quarterly basis, while the fire suppression / detection systems, PDUs, UPS system, and leak detection systems are inspected on a semi-annual or annual basis. Environmental controls are monitored by the data center engineering team 24 hours per day using the BMS. The BMS is configured to send e-mail alert notifications to IT personnel in the event of a device failure and when predefined thresholds are exceeded for certain environmental factors. System events are documented, recorded, and escalated as required. If the problem cannot be immediately resolved by the data center engineering team, it is then escalated to the data center operations manager for further investigation. The data center engineering department has documented escalation procedures for each data center. Additionally, system support technicians and security personnel conduct facility rounds, which include checking environmental control panels and documenting, recording, and escalating system events as required. An incident tracking system is in place to document, record, and escalate environmental system events to help ensure issues are resolved and resolution steps were documented.

London One

Environmental controls are first built on the principle of redundancy. The data center is designed with redundancy for key systems, including Internet data connections, core routers, access and distribution switches, PDUs, dry coolers, CRAC units, and DRUPS systems.

All backup power systems are capable of maintaining continuous system services to the entire center for at least 48 hours without additional fuel. Three independent diesel contractors help ensure delivery before supplies are exhausted.

Processes and systems are implemented to prevent, detect, and mitigate fire damage. The data center is equipped with multi-zoned fire suppression systems, aspirating smoke detectors, heat detectors, fire alarms, fire extinguishers and sprinkler systems in the appropriate areas. Fire drills are completed at least annually to help ensure fire alarms are operating as intended. In regards to leak prevention, 18 inch raised flooring and leak detection systems are utilized in the data server rooms.

Environmental systems are inspected and preventive maintenance is performed at regular intervals in line with manufacturer recommendations. The dry coolers, CRAC units, and DRUPS systems are inspected on an annual basis. Environmental controls are monitored by the data center engineering team 24 hours per day using the BMS. System events are documented, recorded, and escalated as required. If the problem cannot be immediately resolved by the data center engineering team, it is then escalated to the data center operations manager for further investigation. The data center engineering department has documented escalation procedures for each data center.

Additionally, system support technicians conduct facility rounds, which include checking environmental control panels and documenting, recording, and escalating system events as required. An incident tracking system is in place to document, record, and escalate environmental system events to help ensure issues are resolved and resolution steps were documented.

COMPLEMENTARY USER ENTITY CONTROLS

Datapipe's data center 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 data center services to be solely achieved by Datapipe's control activities. Accordingly, user entities 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:

NEW JERSEY ONE AND NEW JERSEY TWO

- 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.

REPORT USE

The description does not omit or distort information relevant to Datapipe's Data Center 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

INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

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 control objectives 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 control objective 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 the Data Center 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.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
All Data Centers			
1.1	Documented policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews the policies and procedures on an annual basis.	Inspected the physical security policies and procedures to determine that documented policies and procedures were in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center and management reviewed the policies and procedures on an annual basis.	No exceptions noted.
1.2	Data center management documents badge access requests on a standardized access request form.	Inspected request forms for a sample of badge access requests processed during the review period to determine that data center management documented badge access requests on a standardized access request form for each badge access request sampled.	No exceptions noted.
1.3	Data center security personnel require badges to be worn at all times.	Observed the physical security access procedures for the in-scope data centers to determine that badges were worn by data center security personnel at all times.	No exceptions noted.
1.4	Physical access to the data center must be authorized before issuing a permanent photo badge.	Inspected request forms for a sample of badge access requests to the in-scope data centers processed during the review period to determine that requests were authorized before issuing a permanent photo badge.	No exceptions noted.
1.5	Security personnel revoke physical access privileges of terminated employees as a component of the employee termination process.	Inspected access reports for a sample of employees terminated during the review period to determine that security personnel revoked physical access privileges for each terminated employee sampled.	No exceptions noted.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.6	Access badges are color-coded to differentiate types of badges.	Observed the physical security access procedures for the in-scope data centers to determine that access badges were color-coded to differentiate types of badges.	No exceptions noted.
1.7	All individuals without a permanent badge are required to sign a visitor log prior to entering the data center.	Observed the visitor access procedures for the in-scope data centers to determine that security personnel required individuals without a permanent badge to sign a visitor log prior to entering each data center.	No exceptions noted.
		Inspected the visitor logs for a sample of months during the review period to determine that visitors signed a visitor log prior to entering the data center for each month sampled.	No exceptions noted.
1.8	Datapipe personnel access to the managed data center rooms is restricted to persons in the following departments: • Directors • Business Operations • Networking • Storage • Inventory Control • Data Center Operations and Security	Inspected the badge access system listing and employee listing to determine that Datapipe personnel access to the managed data center rooms was restricted to persons in the following departments: • Directors • Business Operations • Networking • Storage • Inventory Control • Data Center Operations and Security	No exceptions noted.
1.9	Predefined physical security zones are utilized for the assignment of role-based physical access privileges.	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.	No exceptions noted.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.10	Security personnel are staffed 24 hours per day to monitor physical security controls to the data centers.	Inspected the security officer staffing schedule to determine that security personnel were staffed 24 hours per day to monitor physical security controls to each data center.	No exceptions noted.
1.11	Surveillance cameras are in place to monitor and record activity to and throughout the data center.	Observed the surveillance cameras throughout the in-scope data centers to determine that surveillance cameras were in place to monitor and record activity to and throughout each data center.	No exceptions noted.
1.12	The authentication success and failure of all access attempts are visible and display a picture of enrolled individuals on the officer's workstation.	Observed the physical security authentication procedures for the in-scope data centers to determine that the authentication success and failure of all access attempts were visible and displayed a picture of enrolled individuals on the officer's workstation.	No exceptions noted.
1.13	The electronic badge access system and the biometric access system are configured to log access attempts.	Inspected the badge access system and biometric access system logs for a sample of months during the review period to determine that the electronic badge access system and the biometric access system were configured to log access attempts for each month sampled.	No exceptions noted.
1.14	A third-party security company is contracted to notify Datapipe personnel if unauthorized access is detected.	Inspected the security monitoring service level agreement to determine that a third-party security company was contracted to notify Datapipe personnel if unauthorized access was detected.	No exceptions noted.

Control Objective 1: Physical Security

Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

#	Service Organization's Controls	Service Auditor's Tests	Results of Tests
1.15	Administrative access to the badge access system is restricted to user accounts accessible by security personnel.	Inspected the administrative user listing for the badge access system to determine that administrative access to the badge access system was restricted to user accounts accessible by security personnel.	No exceptions noted.
1.16	Administrative access to the biometric access system is restricted to user accounts accessible by security personnel.	Inspected the administrative user listing for the biometric access system to determine that administrative access to the biometric access system was restricted to user accounts accessible by security personnel.	No exceptions noted.
1.17	Data center security personnel require an authorized ticket from clients prior to granting client contractors access to the client's designated area of the data center.	Inspected request tickets for a sample of client contractor access requests processed during the review period to determine that data center security personnel required an authorized ticket prior to granting client contractors access for each client contractor access request sampled.	No exceptions noted.
1.18	Physical access to the data center must be authorized before issuing a temporary badge.	Inspected tickets for a sample of visitor access requests processed during the review period to determine that temporary physical access to the data center required an authorized ticket for each temporary badge request sampled.	No exceptions noted.
1.19	Security personnel revoke physical access privileges of a client upon receipt of an access revocation request ticket.	Inspected request tickets for a sample of client revocation requests during the review period to determine that security personnel revoked physical access privileges for each client request sampled.	No exceptions noted.

Control Objective 1: Physical Security ***Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.***			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.20	Security personnel review badge access privileges on a semi-annual basis.	Inspected the badge audit report to determine that badge access for each data center was reviewed within the last six months.	No exceptions noted.
London Data Center			
1.21	A mantrap system is in place at the main data center entrance to help restrict access to the data center.	Observed the physical security access procedures to determine that a mantrap system was in place at the main data center entrance to help restrict access to the data center.	No exceptions noted.
1.22	An electronic badge access system is utilized to control access to the data center.	Observed the data center access process to determine that an electronic badge access system was utilized to control access to the data center.	No exceptions noted.
1.23	The main entrance to the data center requires a badge issued by Global Switch.	Observed the physical security access procedures to determine that the main entrance to the data center required a badge issued by Global Switch.	No exceptions noted.
1.24	Two-factor authentication is required to gain access to the managed care suites, which include the following: • Biometric iris verification • PIN code	Observed the physical security access procedures to determine that two-factor authentication was required to gain access to the managed care suites, which included the following: • Biometric iris verification • PIN code	No exceptions noted.

Control Objective 1: Physical Security ***Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.***			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.25	Video archives of the Datapipe Colocation area surveillance camera recordings are retained for at least 90 days.	Inspected the video surveillance camera system configurations and an example historical image generated during the review period to determine that video archives of the Datapipe Colocation area surveillance camera recordings were retained for at least 90 days.	No exceptions noted.
1.26	Video archives of the Global Switch area surveillance camera recordings are retained for at least 30 days.	Inspected the video surveillance camera system configurations and an example historical image generated during the review period to determine that video archives of the Global Switch area surveillance camera recordings were retained for at least 30 days.	No exceptions noted.
New Jersey One and New Jersey Two Data Centers			
1.27	A mantrap system is in place to help restrict access to the following restricted areas: • Main data center entrance • Service entrance • Full managed server rooms • Shipping and receiving area	Observed the physical security access procedures to determine that a mantrap system was in place to help restrict access to the following restricted areas: • Main data center entrance • Service entrance • Full managed server rooms • Shipping and receiving area	No exceptions noted.
1.28	An authorized key request form is required before issuing data center door keys.	Inspected evidence during the review period to determine that security personnel required an authorized key request form before issuing data center door keys.	No exceptions noted.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.29	An electronic badge access system and a biometric access system are utilized to control access to and within the data center.	Observed the electronic badge access system and biometric access system to determine that an electronic badge access system and a biometric access system were utilized to control access to and within the data center.	No exceptions noted.
		Inspected the badge access system and biometric access system listings to determine that an electronic badge access system and a biometric access system were utilized to control access to and within the data center.	No exceptions noted.
1.30	Internal data center doors utilize high security locks and keys.	Observed the internal data center doors to determine that internal data center doors utilized high security locks and keys.	No exceptions noted.
1.31	The security office has a locked security box that contains emergency keys. Key box access is monitored and logged.	Observed the security office within the data center to determine that the security office had a locked security box that contained emergency keys.	No exceptions noted.
		Inspected the key request log generated during the review period to determine that key box access was monitored and logged.	No exceptions noted.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.32	Three-factor authentication is required to gain access to the data center facility main door, which includes the following: • Smart Card • Biometric iris verification • PIN code	Observed the physical security access procedures to determine that three-factor authentication was required to gain access to the data center facility main door, which included the following: • Smart Card • Biometric iris verification • PIN code	No exceptions noted.
1.33	Video archives of surveillance camera recordings are retained for at least 90 days.	Inspected the video surveillance camera system configurations and an example historical image generated during the review period to determine that video archives of surveillance camera recordings were retained for at least 90 days.	No exceptions noted.
Silicon Valley Data Center			
1.34	A mantrap system is in place to help restrict access to the following restricted areas: • Main data center entrance • Full managed server rooms	Observed the physical security access procedures to determine that a mantrap system was in place to help restrict access to the following restricted areas: • Main data center entrance • Full managed server rooms	No exceptions noted.
1.35	An authorized key request form is required before issuing data center door keys.	Inspected evidence during the review period to determine that security personnel required an authorized key request form before issuing data center door keys.	No exceptions noted.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
1.36	An electronic badge access system is utilized to control access to the data center. A biometric iris scan and smartcard reader system are utilized to control access to the managed care suites.	Observed the data center access process to determine that an electronic badge access system was utilized to control access to the data center.	No exceptions noted.
		Observed the data center access process to determine that a biometric iris scan and smartcard reader system were utilized to control access to the managed care suites.	No exceptions noted.
		Inspected the badge access system and biometric access system listings to determine that an electronic badge access system and a biometric iris scan system were utilized to control access to and within the data center.	No exceptions noted.
1.37	Internal data center doors utilize high security locks and keys.	Observed the internal data center doors to determine that internal data center doors utilized high security locks and keys.	No exceptions noted.
1.38	Data center management requires a key request form prior to issuing client equipment keys to customers.	Inspected evidence during the review period to determine that data center management required a key request form prior to issuing client equipment keys to customers.	No exceptions noted.
1.39	The security office has a locked security box that contains emergency keys. Key box access is monitored and logged.	Observed the security office within the data center to determine that the security office had a locked security box that contained emergency keys.	No exceptions noted.

Control Objective 1: Physical Security *Controls provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the key request log generated during the review period to determine that key box access was monitored and logged.	No exceptions noted.
1.40	Three-factor authentication is required to gain access to the data center facility main door, which includes the following: • Smart Card • Biometric iris verification • PIN code	Observed the physical security access procedures to determine that three-factor authentication was required to gain access to the data center facility main door, which included the following: • Smart Card • Biometric iris verification • PIN code	No exceptions noted.
1.41	Video archives of surveillance camera recordings are retained for at least 90 days.	Inspected the video surveillance camera system configurations and an example historical image generated during the review period to determine that video archives of surveillance camera recordings were retained for at least 90 days.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
All Data Centers			
2.1	A documented emergency action procedure is in place to guide personnel in handling environmental security issues.	Inspected the emergency action procedure to determine that a procedure was in place to guide personnel in handling environmental security issues.	No exceptions noted.
2.2	A leak detection system is in place and configured to notify data center personnel in the event that water is detected.	Observed the leak detection system within the in-scope data centers to determine that a leak detection system was in place and configured to notify data center personnel in the event that water is detected.	No exceptions noted.
2.3	Data center equipment is connected to multiple dedicated and redundant power distribution units (PDUs).	Observed the data center PDUs for the in-scope data centers to determine that data center equipment was connected to multiple dedicated and redundant PDUs.	No exceptions noted.
2.4	A third-party vendor inspects and maintains the following fire detection and suppression systems on at least an annual basis: • Audible and visual alarms • Dry pipe pre-action sprinkler system • Fire and smoke detectors • Hand-held fire extinguishers	Inspected the inspection reports to determine that a third-party vendor inspected and maintained the following fire detection and suppression systems during the review period: • Audible and visual alarms • Dry pipe pre-action sprinkler system • Fire and smoke detectors • Hand-held fire extinguishers	No exceptions noted.
2.5	Fire drills are conducted at least annually.	Inspected evidence of the most recent fire drill to determine that fire drills were conducted on an annual basis.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.6	The data center is equipped with multiple dedicated and redundant computer room air conditioner (CRAC) units.	Observed the CRAC units within the in-scope data centers to determine that the data centers were equipped with multiple dedicated and redundant CRAC units.	No exceptions noted.
2.7	The data center is equipped with multiple redundant Internet data connections, core routers, and access and distribution switches.	Inspected the diagram for the Internet connections, core routers, and access and distribution switches to determine that the in-scope data centers were equipped with multiple redundant Internet data connections, core routers, and access and distribution switches.	No exceptions noted.
2.8	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 the environmental monitoring system configurations and an example alert to determine that the system was configured to monitor and automatically generate alerts when predefined environmental thresholds were met.	No exceptions noted.
2.9	The data center production area is maintained on raised flooring.	Observed the data center flooring to determine that the in-scope data center's production area was maintained on raised flooring.	No exceptions noted
2.10	An incident tracking system is in place to document, record, and escalate system events.	Inspected the incident tracking system configuration and an example incident ticket created during the review period to determine that an incident tracking system was in place to document, record, and escalate system events.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
London Data Center			
2.11	A third-party vendor inspects and maintains the DRUPS systems on an annual basis.	Inspected the most recent preventative maintenance inspection reports to determine that a third-party vendor inspected and maintained the DRUPS systems on an annual basis.	No exceptions noted.
2.12	A third-party vendor inspects and maintains the dry cooler and CRAC units on an annual basis.	Inspected the most recent preventative maintenance inspection reports to determine that a third-party vendor inspected and maintained the dry cooler and CRAC units on an annual basis.	No exceptions noted.
2.13	A third-party vendor inspects and maintains the leak detection system on an annual basis.	Inspected the most recent preventative maintenance inspection reports to determine that a third-party vendor inspected and maintained the leak detection system on an annual basis.	No exceptions noted.
2.14	Multiple DRUPS systems are in place to provide electricity to the data center in the event of a power outage.	Observed the DRUPS systems within the data center to determine that multiple DRUPS systems were in place.	No exceptions noted.
2.15	System support technicians perform reviews of environmental systems at least two times per day to ensure systems are functioning properly.	Inspected the facilities shift schedule and the internal facility rounds reports for a sample of dates during the review period to determine that system support technicians performed reviews of environmental systems at least two times per day.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.16	The data center is equipped with multiple dedicated and redundant dry coolers.	Observed the data center dry coolers to determine that the data center was equipped with multiple dedicated and redundant dry coolers.	No exceptions noted.
2.17	The data center is protected by fire detection and suppression controls that include, but are not limited to, the following: • Audible and visual alarms • INERGEN gas suppression system • VESDA fire and smoke detectors • Hand-held fire extinguishers	Observed the fire detection and suppression equipment within the data center to determine that the data center was protected by fire detection and suppression controls that included the following: • Audible and visual alarms • INERGEN gas suppression system • VESDA fire and smoke detectors • Hand-held fire extinguishers	No exceptions noted.
New Jersey One and New Jersey Two Data Centers			
2.18	A third-party vendor inspects and maintains the generators on a quarterly basis.	Inspected preventative maintenance inspection reports for a sample of quarters during the review period to determine that a third-party vendor inspected and maintained the generators on a quarterly basis.	No exceptions noted.
2.19	A third-party vendor inspects and maintains the UPS systems on a semi-annual basis and the PDUs on an annual basis.	Inspected the most recent preventative maintenance inspection reports to determine that a third-party vendor inspected and maintained the UPS systems on a semi-annual basis and the PDUs on an annual basis.	No exceptions noted.
2.20	Backup power systems are capable of maintaining continuous system services to the data center for at least 72 hours without additional fuel.	Observed the data center and inspected maintenance reports to determine that backup power systems were capable of maintaining continuous system services to the data center for at least 72 hours without additional fuel.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.21	Data center equipment is connected to multiple redundant UPS systems to provide temporary electricity in the event of a power outage.	Observed the UPS systems within the data center to determine that data center equipment was connected to multiple redundant UPS systems to provide temporary electricity in the event of a power outage.	No exceptions noted.
2.22	Datapipe personnel inspect and maintain the CRAC units on a quarterly basis.	Inspected the preventative maintenance inspection reports for a sample of quarters during the review period to determine that Datapipe personnel inspected and maintained each CRAC unit on a quarterly basis.	No exceptions noted.
2.23	Datapipe personnel inspect and maintain the leak detection system on an annual basis.	Inspected the most recent internal preventative maintenance inspection report to determine that Datapipe personnel inspected and maintained the leak detection system on an annual basis.	No exceptions noted.
2.24	Documented policies and procedures are in place to guide employees in the maintaining and monitoring of the environmental equipment supporting the data center.	Inspected the environmental controls policy to determine that documented policies and procedures were in place to guide employees in the maintaining and monitoring of the environmental equipment supporting the data center.	No exceptions noted.
2.25	Multiple dedicated generators are in place to provide electricity to the data center in the event of a power outage.	Observed the data center generators to determine that multiple dedicated generators were in place to provide electricity to the data center in the event of a power outage.	No exceptions noted.
2.26	Security personnel perform reviews of environmental systems at least eight times per day to ensure systems are functioning properly.	Inspected the facilities shift schedule and the internal facility rounds reports for a sample of dates during the review period to determine that security personnel performed reviews of environmental systems at least eight times per day.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.27	The data center is protected by fire detection and suppression controls that include, but are not limited to, the following: • Audible and visual alarms • A dual interlocking dry-pipe pre-activation sprinkler system with heat detectors • VESDA fire and smoke detectors • Hand-held fire extinguishers	Observed the fire detection and suppression equipment within the data center to determine that the data center was protected by fire detection and suppression controls that included the following: • Audible and visual alarms • A dual interlocking dry-pipe pre-activation sprinkler system with heat detectors • VESDA fire and smoke detectors • Hand-held fire extinguishers	No exceptions noted.
2.28	The environmental monitoring application is configured to send email alert notifications to IT personnel in the event of a device failure and when predefined thresholds are exceeded for certain environmental factors.	Inspected the environmental monitoring application alert notification configuration and an example e-mail alert notification generated during the review period to determine that the environmental monitoring application was configured to send email alert notifications to IT personnel in the event of a device failure and when predefined thresholds were exceeded for certain environmental factors.	No exceptions noted.
Silicon Valley Data Center			
2.29	A third-party vendor inspects and maintains the DRUPS systems on a quarterly basis.	Inspected preventative maintenance inspection reports for a sample of quarters during the review period to determine that a third-party vendor inspected and maintained the DRUPS systems on a quarterly basis.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.30	A third-party vendor inspects and maintains the UPS system and PDUs on a semi-annual basis.	Inspected the most recent preventative maintenance inspection reports to determine that a third-party vendor inspected and maintained the UPS system and PDUs on a semi-annual basis.	No exceptions noted.
2.31	Backup power systems are capable of maintaining continuous system services to the entire data center for at least 48 hours without additional fuel.	Observed the data center and inspected maintenance reports to determine that backup power systems were capable of maintaining continuous system services to the data center for at least 48 hours without additional fuel.	No exceptions noted.
2.32	Data center equipment is connected to a UPS system to provide temporary electricity in the event of a power outage.	Observed the UPS system within the data center to determine that data center equipment was connected to a UPS system to provide temporary electricity in the event of a power outage.	No exceptions noted.
2.33	Datapipe personnel inspect and maintain the CRAC units on a quarterly basis.	Inspected the preventative maintenance inspection reports for CRAC units for a sample of quarters during the review period to determine that Datapipe personnel inspected and maintained each CRAC unit on a quarterly basis.	No exceptions noted.
2.34	Datapipe personnel inspect and maintain the leak detection system on an annual basis.	Inspected the most recent internal preventative maintenance inspection report to determine that Datapipe personnel inspected and maintained the leak detection system on an annual basis.	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.35	Documented policies and procedures are in place to guide employees in the maintaining and monitoring of the environmental equipment supporting the data center.	Inspected the environmental controls policy to determine that documented policies and procedures were in place to guide employees in the maintaining and monitoring of the environmental equipment supporting the data center.	No exceptions noted.
2.36	Equipment within the data center is placed on racks to protect the infrastructure from localized flooding.	Observed the equipment racks within the data center to determine that equipment within the data center was placed on racks to protect the infrastructure from localized flooding.	No exceptions noted.
2.37	Multiple DRUPS systems are in place to provide electricity to the data center in the event of a power outage.	Observed the DRUPS systems within the data center to determine that multiple DRUPS systems were in place.	No exceptions noted.
2.38	System support technicians and security personnel perform reviews of environmental systems two times per day to ensure systems are functioning properly.	Inspected the facilities shift schedule and the internal facility rounds reports for a sample of dates during the review period to determine that system support technicians and security personnel performed reviews of environmental systems two times per day.	No exceptions noted.
2.39	The data center is protected by fire detection and suppression controls that include, but are not limited to, the following: • Audible and visual alarms • A single interlocking dry-pipe pre-activation sprinkler system with heat detectors • VESDA fire and smoke detectors • Hand-held fire extinguishers	Observed the fire detection and suppression equipment within the data center to determine that the data center was protected by fire detection and suppression controls that included the following: • Audible and visual alarms • A single interlocking dry-pipe pre-activation sprinkler system with heat detectors • VESDA fire and smoke detectors • Hand-held fire extinguishers	No exceptions noted.

Control Objective 2: Environmental Security *Controls provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.*			
#	**Service Organization's Controls**	**Service Auditor's Tests**	**Results of Tests**
2.40	The environmental monitoring application is configured to send email alert notifications to IT personnel in the event of a device failure and when predefined thresholds are exceeded for certain environmental factors.	Inspected the environmental monitoring application alert notification configuration and an example e-mail alert notification generated during the review period to determine that the environmental monitoring application was configured to send email alert notifications to IT personnel in the event of a device failure and when predefined thresholds were exceeded for certain environmental factors.	No exceptions noted.